Vysoká škola báňská – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Monitoring a analýza provozu bezdrátových sítí

Monitoring and Traffic Analysis of Wireless Networks

2015 Václav Durčík

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Zadání bakalářské práce

Student: **Václav Durčík**

Studijní program: B2647 Informační a komunikační technologie

Studijní obor: 2612R059 Mobilní technologie

Téma: Monitoring a analýza provozu bezdrátových sítí
Monitoring and Traffic Analysis of Wireless Networks

Zásady pro vypracování:

Pomocí bezdrátové sítě je možné propojit jednotlivé počítače, nebo umožnit sdílení jiných zdrojů ostatním počítačům, např. tiskárny, kamery a podobně. S Narůstajícím počtem zařízení v bezdrátových sítích roste i potřeba monitoringu těchto sítí. Následnou analýzou provozu lze odhalit bezpečnostní rizika. Cílem práce bude popsat bezdrátové sítě a možnosti sledování a analýzy provozu v těchto sítích.

1. Popište standardy pro bezdrátové sítě se zaměřením na technologie 802.11.
2. Vyberte a otestujte alespoň tři různé open source nástroje pro monitoring a analýzu provozu v bezdrátových sítí.
3. Použijte nástroj Kismet pro monitoring a analýzu provozu a porovnejte jej s Vámi vybranými nástroji.
4. Z výsledku testování vyhodnoťte použití jednotlivých nástrojů pro sledování a analýzu provozu.

Pro vypracování závěrečné práce bude použit typografický systém LaTeX.

Seznam doporučené odborné literatury:

RACKLEY, Steve, Michael J SCHEARER a Frank THORNTON. *Wireless networking technology: from principles to successful implementation*. 3rd Ed. Boston: Elsevier, Newnes, 2007, ix, 413 p. ISBN 07-506-6788-5.

WRIGHTSON, Tyler, Michael J SCHEARER a Frank THORNTON. *Wireless network security: a beginner's guide*. 3rd Ed. New York: McGraw-Hill, c2012, xvii, 347 p. ISBN 00-717-6094-6.

HAINES, Brad, Michael J SCHEARER a Frank THORNTON. *Kismet hacking: all-in-one next-generation firewall, IPS, and VPPN services*. 3rd Ed. Burlington, MA: Syngress Publishing, Inc., c2008, xi, 258 p. ISBN 978-159-7491-174.

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Miroslav Bureš**

Datum zadání: 01.09.2014

Datum odevzdání: 07.05.2015

doc. Ing. Miroslav Vozňák, Ph.D.
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě 7. května 2015 .....

Rád bych na tomto místě poděkoval panu Ing. Miroslavu Burešovi za rady a odbornou pomoc při tvorbě této bakalářské práce.

Abstrakt

Tato práce je zaměřena na monitoring a analýzu bezdrátových síti se zaměřením na technologie standardu 802.11. Práce zahrnuje odborný popis uvedeného Wi-Fi standardu IEEE 802.11, který je zahrnut mezi WLAN sítě. Cílem práce je popsat bezdrátové sítě a možnosti sledování a analýzy provozu v těchto sítích pomocí open-source programů pro to určené.

Klíčová slova: WIFI, bezdrátové sítě, monitoring sítí, analýza sítí, sniffer, IEEE 802.11

Abstract

This work is focused on the monitoring and analysis of wireless network technology with a focus on 802.11. The work includes a description of the Wi-Fi IEEE 802.11, which is included among the WLAN network. The aim is to describe wireless networks, and the monitoring and analysis of traffic on these networks using open-source programs for this.

Keywords: WIFI, wireless networks, network monitoring, network analysis, sniffer, IEEE 802.11

Seznam použitých zkratek a symbolů

AES	–	Advanced Encryption Standard
AP	–	Access Point
BSA	–	Basic Service Area
BSS	–	Basic Service Set
CRC	–	Cyclic Redundancy Check
CCMP	–	Counter Cipher Mode with Block Chaining Message Authentication Code Protocol, CCM mode Protocol
ČTU	–	Český telekomunikační úřad
DCF	–	Distributed Coordination Function
DES	–	Data Encryption Standard
DS	–	Distribution System
DSSS	–	Direct Sequence Spread Spectrum
EAP	–	Extensible Authentication Protocol
EIRP	–	Equivalent Isotropically Radiated Power, Effective Isotropic Radiated Power
ESS	–	Extended Service Set
FCS	–	Frame Check Sequence
FFC	–	The Federal Communications Commission
FHSS	–	Frequency-Hopping Spread Spectrum
GTK	–	Group Temporal Key
GUI	–	Graphical User Interface
HORST	–	Highly Optimized Radio Scanning Tool
IBSS	–	Independent Basic Service Set
ISM	–	Industrial, Scientific and Medical radio bands
LLC	–	Logical Link Control
MAC	–	Media Access Control
MIC	–	Message authentication code
MIMO	–	Multiple-Input and Multiple-Output
MU-MIMO	–	Multi-User Multiple-Input and Multiple-Output
NAV	–	Network Allocation Vector
NETSH	–	Network Shell
NIST	–	National Institution of Standards and Technology
NSA	–	National Security Agency

OFDM	–	Orthogonal Frequency-Division Multiplexing
PCF	–	Port Coordination Function
PLCP	–	Physical Layer Convergence Procedure, Protocol
PMD	–	Physical Medium Dependent
PSK	–	Pre-shared key
PTK	–	Pairwise Transient Key
QAM	–	Quadrature Amplitude Modulation
RC4	–	Ron's Code 4
RTS/CTS	–	Request To Send / Clear To Send
SISO	–	Single-Input Single-Output
SSID	–	Service Set Identifier
SU	–	Single-User
SU-MIMO	–	Single-User Multiple-Input and Multiple-Output
TKIP	–	Temporal Key Integrity Protocol
WEP	–	Wired Equivalent Privacy
WIFI	–	Wireless Fidelity
WiGig	–	Wireless Gigabit Alliance
WLAN	–	Wireless Local Area Network
WPA	–	Wi-Fi Protected Access

Obsah

Seznam tabulek

Seznam obrázků

Seznam výpisů zdrojového kódu

Úvod

V dnešní době jsou hodně populární bezdrátové sítě. A to jak digitální vysílaní (DVB-T), různá rádia a nebo bezdrátové sítě WLAN působících v bezlicenčních pásmech ISM 2,4 a 5 GHz jimiž se tato práce zabývá.

Pomocí bezdrátové sítě je možné propojit jednotlivé počítače, nebo umožnit sdílení jiných zdrojů ostatním počítačům, např. tiskárny, kamery a podobně. S narůstajícím počtem zařízení v bezdrátových sítích roste i potřeba monitoringu těchto sítí. Následnou analýzou provozu lze odhalit bezpečnostní rizika.

V úvodní kapitole se tato práce zabývá popisem standartu IEEE 802.11 od její historie až po současnost. V kapitole jsou taky popsány základní pojmy, různé typy sítí, frekvenční pásma, řešení fyzické a linkové vrstvy a způsoby zabezpečení ve WI-FI sítích.

Dále se tato práce zabývá open-source nástroji pro monitoring a analýzu bezdrátových sítí. U každého zvoleného nástroje jsou uvedeny jeho možnosti z hlediska sledování a analýzy sítě. Naměřené a zjištěné výsledky z výstupu programů jsou porovnány s programem KISMET.

V části zabývající monitoringem a analýzou bezdrátových sítí, jsou popsány realizovatelné postupy sledování a analýzy sítě, včetně praktických ukázek.

V poslední části této práce je uvedeno vyhodnocení výsledků testování a vyhodnocení použití jednotlivých nástrojů pro sledování a analýzu provozu.

1 Standard IEEE 802.11

1.1 Historie standardu IEEE 802.11 [17]

Technologie IEEE 802.11 má svůj původ v roce 1985 rozhodnutí ze strany Federal Communications Commission USA, která uvolnila ISM pásma pro bezlicenční použití.

První bezdrátové technologie se objevily v roce 1990 a pracovaly v kmitočtovém pásmu 900 MHz s rychlostí 1 Mb/s (mnohem pomalejší než kabelové sítě LAN, které v té době byly schopné přenášet data až 10 Mb/s).

V roce 1991 NCR Corporation / AT&T (nyní Alcatel-Lucent a LSI Corporation) vynalezla předchůdce standardu 802.11 v Nieuwegeinu (Nizozemsko). Původně měla být technologie použita pro pokladní systémy. První bezdrátové produkty byly uvedeny na trh pod obchodním názvem WaveLAN s datovými rychlostmi 1 Mbit/s a 2 Mbit/s.

V roce 1999 vznikla obchodní asociace tzv. Wi-Fi Alliance. Vytvořila se obchodní značka Wi-Fi, pod kterou se dnes většina výrobků prodávají.

Standard	Rok vydání	Maximální přenosová rychlost [MBit/s]	Frekvenční pásmo [GHz]	Fyzická vrstva
IEEE 802.11	1997	2	2,4	FHSS nebo DSSS
IEEE 802.11b	1999	11	2,4	DSSS
IEEE 802.11a	1999	54	5	OFDM
IEEE 802.11g	2003	54	2,4	OFDM
IEEE 802.11n	2009	6000	2,4 a 5	OFDM, MIMO
IEEE 802.11ac	2013	1300	5	256-QAM, MU-MIMO, OFDM
IEEE 802.11ad	2014	7000	2,4; 5 a 60	

Tabulka 1.1: Přehled standardů IEEE 802.11

1.2 Popis standardů IEEE 802.11 [17]

Projekt IEEE 802.11 začal vyvíjet v roce 1990 a byl schválen v roce 1997. Cílem 802.11 bylo vyvinout standard k řízení přístupu k médiu (MAC) a fyzické (PHY) vrstvy pro stolní, přenosné a mobilní bezdrátové zařízení.

Standard je používán v 2,4 GHz bezlicenčním pásmu a maximální přenosová rychlost je 2 MBit/s. Z hlediska přenosové rychlosti jsou na fyzické vrstvě používané tyto technologie:

- **FHSS** - 1 Mbit/s nebo 2 Mbit/s (viz kap.1.6.1)

- **DSSS** - 1 Mbit/s nebo 2 Mbit/s (viz kap. 1.6.2)
- **IR** - 1 Mbit/s

1.2.1 Standard IEEE 802.11b

V roce 1999 byl definován standard 802.11b, který pracuje v bezlicenčním pásmu 2,4 GHz. V standardu se zlepšily modulační systémy, které přinesly vyšší rychlosti přenosu.

Původní standard 802.11 byl omezen na přenosové rychlosti 1 a 2 Mb/s. 802.11b podporuje přenosové rychlosti 5,5 a 11 Mb/s. Stejně jako lepší rychlost přenosu dat, 802.11b také začal používat Wired Equivalent Privacy - **WEP** (viz. kap. 1.9.3), který podporoval kryptografické zabezpečení sítě. Na fyzické vrstvě je použita technika přímého rozprostřeného spektra (**DSSS**) viz. kap. 1.6.2.

1.2.2 Standard IEEE 802.11a

V roce 1999 byl taky představen standard 802.11a. Pracuje v 5 GHz pásmu, které je oproti 2,4 GHz pásmu méně rušeno zařízeními jako Bluetooth, mikrovlnnými troubami nebo některými radioamatérskými bezdrátovými stanicemi.

Maximální přenosová rychlost se zvedla na 54Mbit/s, ale může se přizpůsobit na rychlosti 8, 36, 24, 18, 12, 9 nebo 6 Mb/s v závislosti na podmínkách použitého kanálu. Na fyzické vrstvě je použit ortogonální multiplex s frekvenčním dělením **OFDM** (viz. kap. 1.6.3).

1.2.3 Standard IEEE 802.11g

Když v roce 2001 **FFC** (The Federal Communications Commission) povolila použití **OFDM** (viz. kap. 1.6.3), byl v roce 2003 představen další standard 802.11g. Stejně jako standard 802.11a, 802.11g podporuje přenosové rychlosti až do 54 Mb/s.

Pracuje 2,4 GHz pásmu (jako 802.11b) a musí být zpětně kompatibilní se zařízeními 802.11b. Proto tento standard provozuje řadu ochranných mechanismů, aby mohl koexistovat se zařízeními 802.11b.

1.2.4 Standard IEEE 802.11n

K vetším změnám došlo v roce 2009 kdy byl představen standard 802.11n. Předchozí standardy vylepšuje použitím **MIMO** technologie tzn. bylo použito více antén pro příjem a vysílání signálu (viz.kap 1.6.4). Na spojové vrstvě (MAC) došlo k zlepšení agregaci rámců a blokového spojování.

Standard pracuje jak 2,4 GHZ bezlicenčním pásmu, tak i 5 GHz a je zpětně kompatibilní s předchozími standardy. Používá šířku kanálu 20 MHz jedním streamem (72 MB/s) nebo dvojnásobnou šířku kanálu 40 MHz (150 MB/s). Přenosová rychlost se zvedla až na 600 MBit/s. 802.11n stále používá **OFDM**, ale uvádí řadu vylepšení např.:

- více subnosných

- kratší ochranné intervaly
- lepší kanálové spojení
- použití modulace signálu - 64 QAM

1.2.5 Standard IEEE 802.11ac

V roce 2013 byl představen standard 802.11ac, který staví na 802.11n. Přenosová rychlost je až do 1GBit/s.

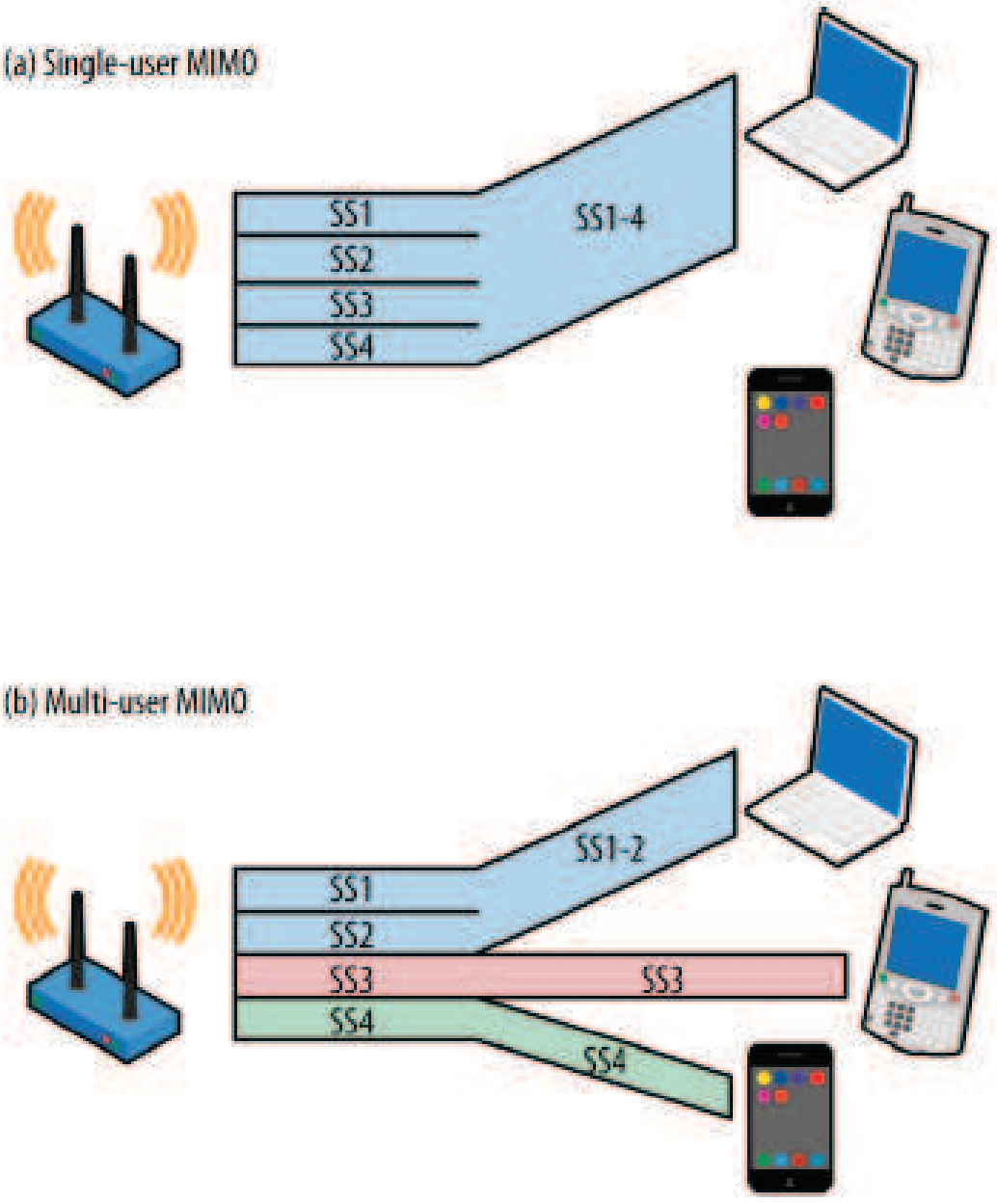
802.11n	**802.11ac**
Podpora 20 a 40 MHz kanálů	Přidány 80 a 160 MHz kanály
Podpora 2,4 GHz a 5 GHz frekvenčních pásmem	Podporuje pouze 5 GHz frekvenční pásmo
Podpora BPSK, QPSK, 16-QAM a 64-QAM	Přidána 256-QAM
Podpora mnoho typů explicitního beamformingu (tvarování paprsku)	Podpora pouze nulového datového paketu (NDP) explicitního beamformingu
Podporuje až čtyři prostorové proudy (spatial streams)	Podporuje až osm prostorových proudů (AP); u klientských zařízení až čtyři prostorové proudy
Podpora pouze single-user vysílání	Přidáno multi-user vysílaní
Obsahuje významné vylepšení MAC (A-MSDU, A-MPDU)	Podpora podobného vylepšení MAC, ale s rozšířením přizpůsobit se vysokým rychlostem přenosu dat

Tabulka 1.2: Rozdíly mezi 802.11n a 802.11ac

802.11ac představuje dvě nové velikosti kanálu: **80** MHz a **160** MHz. Stejně jako u 802.11n širší kanály zvyšují rychlost přenosu. Větší šířka kanálu, ale taky přináší problém s vetším zahuštěním pásma. Standard tak představuje dvě formy 160 MHz kanálu: jeden 160 MHz blok a nebo 80 + 80 MHz kanál, který kombinuje dva 80 MHz kanály a poskytuje stejnou funkci.

Standard používá **256 QAM** modulaci. Použitím složitější modulace, který podporuje více datových bitů, je možné vyslat osm bitů za jednou periodu. Tohle přineslo zisk 30 procent.

Před 802.11ac byly standardy 802.11 **Single-User**: každé vysílané pakety byly poslány jednomu cíli. Tak hlavní změna nastala v použití **MU-MIMO** (multi-user multiple-input and multiple-output) technologie. MU-MIMO je schopnost přístupového bodu vysílat několika klientům současně (viz. obr. 1.1).



Obrázek 1.1: Rozdíly mezi SU-MIMO a MU-MIMO

1.2.6 Standard IEEE 802.11ad

Následujícím standardem je 802.11ad. Na vzniku se podílí aliance WiGig. Pracuje nově i v 60 GHz pásmu, které má odlišné vlastnosti šíření, než pásma 2,4 Ghz a 5 Ghz. Tato technologie je určena pro sítě, které jsou malého dosahu. Způsobuje to použitím velkého kmitočtového pásma, a proto rádiové vlny velmi špatně pronikají překážkami. Vrcholová přenosová rychlost je do 7 GBit/s.

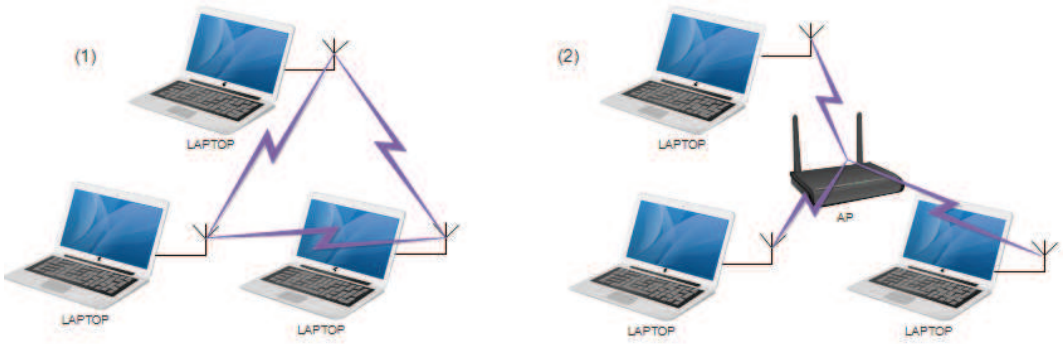
1.3 Typy sítí [7]

Wi-Fi architektura je velmi flexibilní, což umožňuje značnou mobilitu stanic a transparentní integraci s kabelovými sítěmi IEEE.

Základním stavebním prvkem sítí 802.11 je **BSS** (Basic Service Set). BSS je skupina stanic, které jsou logicky navzájem spojeny, a které mezi sebou komunikují.

Komunikace BSS probíhá v rámci oblasti tzv. **BSA** (Basic Service Area) definovaná vlastnostmi šíření bezdrátového média. Pokud stanice je v základní oblasti služeb (BSS), může komunikovat s ostatními členy BSS. Komunikaci mezi BSS může rozdělit do dvou základních konfiguraci:

- Nezávislé sítě ad hoc
- Infrastrukturní sítě



Obrázek 1.2: Nezávislá ad hoc (1) a infrastrukturní síť (2)

1.3.1 Ad hoc sítě

Nezávislé ad hoc sítě jsou označovány jako **IBSS** (Independent Basic Service Set). Stanice v IBSS komunikují navzájem přímo mezi sebou a musí být v přímém dosahu komunikace. Nejmenší možná realize v síti 802.11 je IBSS s dvěma stanicemi. Nezávislé stanice IBBS se typicky skládají z malého počtu stanic pro konkrétní účel a vetšinou na krátkou dobu provozu. Jedno z běžných použití je vytvoření „**short-lived**"sítě s podporou jednoho setkání v síti (v konferenční místnosti). Na začátku účastníci vytvoří IBSS ke sdílení dat

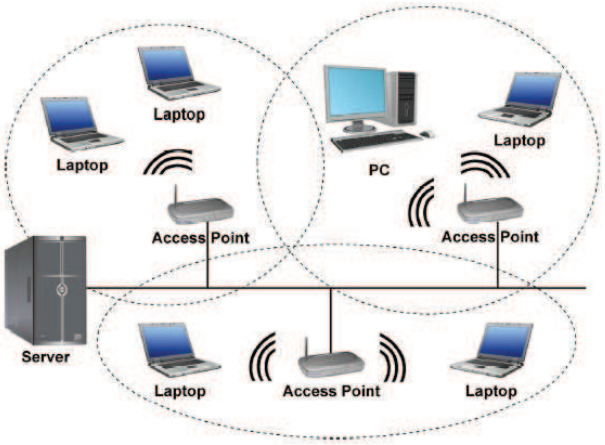
a pak probíhá komunikace. Na konci setkání je IBSS odstraněno. U této sítě je nutnost dodržet správnou konfigurace jednotlivých zúčastněných stanic.

Obrázek 1.3: Příklad nezávislé ad hoc sítě

1.3.2 Infrastrukturní sítě

Infrastrukturní sítě se vyznačují použitím přístupového bodu (AP). Přístupové body jsou používány pro veškerou komunikaci v sítí infrastruktury, včetně komunikace mezi mobilními uzly ve stejné oblasti služeb. Jednotlivé stanice komunikují přes prostředníka (AP), který funguje jednak jako vysílač a jednak jako datový most. Původní mobilní stanice přenáší rámce k přístupovému bodu a přístupový bod přenáší rámce na cílové stanici. I když tato realizace sítě způsobuje větší přenosovou kapacitu než posílání rámců přímo (odesílatel - příjemce), má i své výhody:

- BSS infrastruktura je definována podle vzdálenosti od přístupového bodu. Všechny mobilní stanice musí být v dosahu přístupového bodu, ale žádné omezení se netýká vzdálenosti mezi jednotlivými mobilními stanicemi. Povolení přímé komunikace mezi mobilními stanicemi by se ušetřila přenosová kapacita, ale za cenu zvýšení složitosti fyzické vrstvy, protože mobilní stanice budou muset udržovat vztahy (komunikaci) mezi sebou.
- Přístupové body v infrastrukturních sítí jsou na pozici, která napomáhá jednotlivým stanicím k úsporám energie.



Obrázek 1.4: Příklad infrastrukturní sítě

1.4 Frekvenční pásma

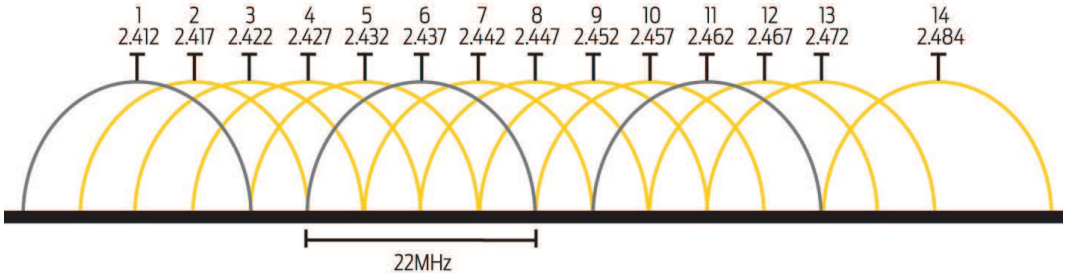
ISM (Industrial, Scientific and Medical) jsou bezlicenční pásma, ale nejsou nijak chráněna proti rušení. Tyto pásma využívají několik oborů např. průmyslové, vědecké nebo zdravotnické. Běžné WIFI sítě pracují ve dvou bezlicenčních pásmech ISM:

- 2,4 GHz
- 5 GHz

1.4.1 Frekvenční pásmo 2,4 GHz

V bezlicenční pásmo 2,4 GHz využívají standarty 802.11, 802.11b, 802.11g. Na této frekvenci pracuje velké množství zařízení např. mikrovlnná trouba, které mohou rušit vysílaný signál. Tento problém vyřešil přechod do vyššího frekvenčního pásma 5 GHz.

V pásmu je definováno 14 kanálů, které mají odstup 5 MHz. Maximální hodnota **EIRP** (Equivalent Isotropically Radiated Power, Effective Isotropic Radiated Power) v České republice je 100 mW (20 dBm).



Obrázek 1.5: Rozdělení kanálů v 2,4 GHz pásmu

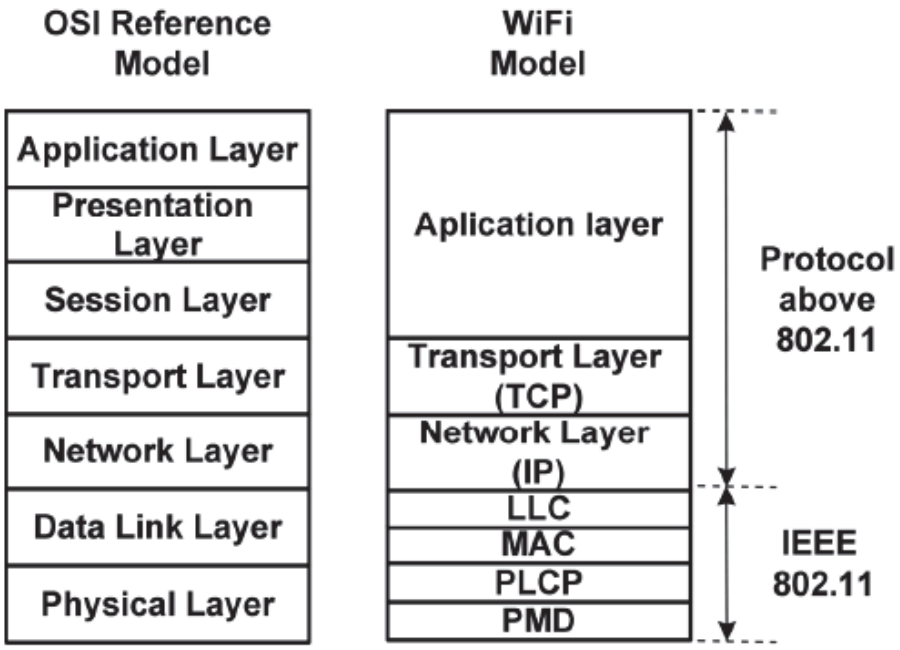
Na obrázku 1.5 lze vidět, že některé kanály se navzájem překrývají. Proto při konfiguraci bezdrátové sítě je třeba dbát na tento problém.

1.4.2 Frekvenční pásmo 5 GHz [7]

Použitím 5 GHz bezlicenčního pásma se vyřešil problém 2,4 GHz, kde docházelo k většímu rušení signálu jinými zařízeními pracující na stejné frekvenci. V Evropě je dostupných 19 kanálů s odstupem 20 MHz. V České republice je prvních 8 kanálů vyhrazeno pro vnitřní použití budov s maximálním výkonem EIRP = 200mW. Zbylých 11 kanálů lze použít i mimo budovy (max. EIRP = 1 W), ale na vysílacích zařízení musí být zajištěna možnost regulace výstupního výkonu. Pásmo 5 GHZ využívají standarty 802.11a, 802.11n, 802.11ac, 802.11ad.

1.5 Protokolová architektura

Standard IEEE 802.11 definuje spojovou a fyzickou vrstvu modelu OSI.



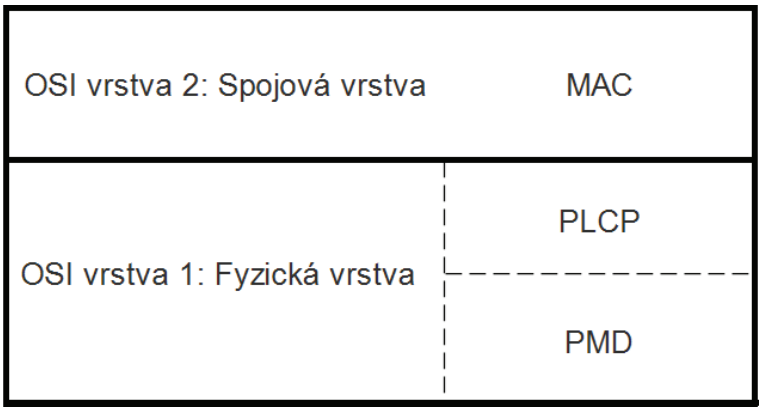
Obrázek 1.6: Protokolová architekrura

1.6 Fyzická vrstva [7]

Fyzická vrstva je rozdělena do dvou podvrstev:

- **PLCP** (Physical Layer Convergence Protocol,Procedure) - Podvrstva PLCP mapuje MAC rámce na přenosovém médiu. Poskytuje rozhraní pro PMD. Obsahuje informace např. o síle signálu či použitém kanálu.

- **PMD** (Physical Media Dependent) - Tato podvrstva je odpovědná za přenos bitů, které obdrží od PLCP do „vzduchu"pomocí antény. PMD zajišťuje kódování a modulaci signálu.



Obrázek 1.7: Fyzická s spojová vrstva - logická architektura

Fyzická vrstva tedy definuje typ použité modulace (QPSK, BPSK, 16-QAM a 64-QAM) a použitou techniku spektra. U standardů 802.11 se využívají tři různé techniky rozprostřeného spektra: **FHSS**, **DSSS** a **OFDM**.

1.6.1 FHSS

Princip frekvenčního přeskakování **FHSS** (Frequency Hopping Spread Spectrum) spočívá v přeskakování z jedné frekvence na druhou při přenosu informací (bitů). Tuto metodu můžeme rozdělit do dvou skupin:

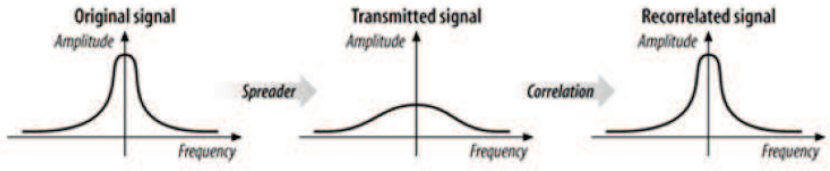
- **Fast Hopping** (FFH)- Rychlé skákání během přenosu bitu mění jednou nebo vícekrát frekvence tzn. více přeskoků za přenesený bit.
- **Slow Hopping** (SFH)- Při pomalém přeskakování je přeneseno několik bitů a poté se změní frekvence. Používá se pro rychlé rychlosti přenosu dat, protože frekvenční syntezátory ve vysílači a přijímači nejsou schopny přejít a usadit se na nové frekvence dostatečně rychle, aby se udržel krok s rychlostí přenosu dat, pokud se přenáší jeden nebo méně bitů na jednom přeskoku.

U frekvenčního přeskakování je pásmo (2,4 GHz) rozděleno za 79 kanálů a každý z nich má šířku 1MHz. Na každém kanále dochází k vysílání (přenos dat) 400ms a minimálně dojde k 2,5x přeskokům než se změní frekvence. Tímto se snižuje případný vliv rušení signálu. Tuto techniku rozprostření spektra využívá standard IEEE 802.11.

1.6.2 DSSS

Přímá sekvence rozprostření spektra **DSSS** (Direct Sequence Spread Spectrum) - signál je rozprostřen do většího pásma. Každý jednotlivý bit při přenosu dat je nahrazen sekvencí

jednoho nebo více bitů (chipů), které mají pseudonáhodný charakter. Sekvence bitů tvoří např. Goldovy nebo Barkerovy kódy. Bitová rychlost tohoto kódu je mnohem vyšší, než je bitová rychlost informačních dat, takže šířka pásma RF signálu je tedy vyšší, než je šířka pásma dat. DSSS může poskytnout vyšší rychlost přenosu dat s menší redundancí než je to u FHSS.



Obrázek 1.8: Princip DSSS

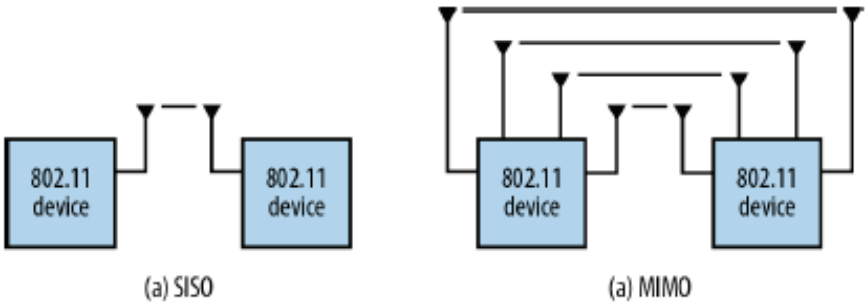
1.6.3 OFDM

Ortogonální multiplex s frekvenčním dělením **OFDM** (Orthogonal Frequency Division Multiplex) rozděluje dostupný kanál do několika subkanálů a kóduje část signálu přes každý dílčí kanál paralelně. Signál je vysílán na více vzájemně ortogonálních frekvencích, kterým říkáme subnosné. Subnosné jsou dále podle potřeby modulovány modulacemi např. QPSK, 16-QAM, 64-QAM nebo 256-QAM. Tuto metodu využívají standardy 802.11a/g/n/ac.

1.6.4 SISO a MIMO

Před **MIMO** (multiple-input, multiple-output) byl u standardů 802.11 používán jeden datový tok (data stream) - vysílač a přijímač používá jednu anténu. Tento komunikační systém je nazýván **SISO** (Single-Input/Single-Output). Je nutno podotknout, že standardy 802.11 podporují obousměrnou střídavou komunikaci (half-duplex).

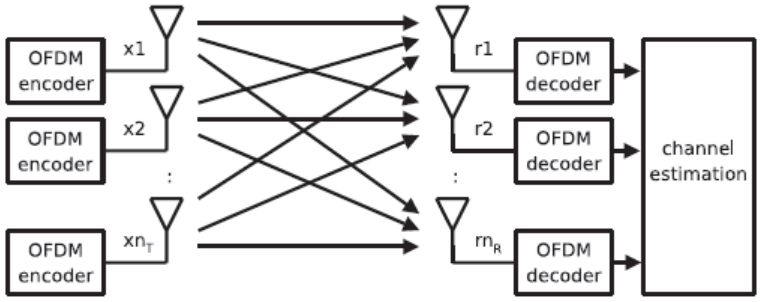
Poznámka 1.1 Half-duplex - V daném okamžiku může probíhat komunikace v jednom směru, směr přenosu dat se může dle potřeby měnit.



Obrázek 1.9: Rozdíl mezi SISO a MIMO

Multiple-input, multiple-output (MIMO) je technologie pro velké datové rychlosti přenosu dat. MIMO systémy se skládají z více antén a RF řetězců u vysílače a přijímače (viz obr. 1.10). Počet antén / RF řetězců ve vysílači (nT), nemusí být stejné jako číslo v přijímači (nR). Technologie MIMO je prospěšná pro OFDM systémy, které přenáší signály ve více úzkopásmových kanálech. MIMO-OFDM je tedy výhodná pro výzkum vysokorychlostních bezdrátových systémů.

MIMO systémy přinesly zvýšení kapacity prostřednictvím prostorové diverzity a prostorového multiplexování. Prostorová diverzita (Spatial diversity) existuje ve dvou formách: přijímací a vysílací. Antény na vysílačích nebo přijímačích jsou od sebe vzdáleny tak, aby každá anténa dostala nekorelovaný signál. Jednoduše řečeno, anténa s nejlepším signálem je vybrána pro zpracování RF řetězcem.



Obrázek 1.10: MIMO komunikační systém

1.6.5 Beamforming

Beamforming neboli tvarování paprsku je metoda, která umožňuje řízení směrování a tvar vysílaného nebo přijímaného signálu v MIMO systémech pomocí senzorových polí v kombinaci s technikami zpracování signálu (zajišťuje formátování signálu, aby k přijímači došel co v nejlepší kvalitě). Tato metoda je použita u standardů 802.11n a vyšší.

1.7 Linková vrstva [7]

Standard 802.11 definuje na spojové linkové vrstvě ve podvrstvy:

- **LLC** (Logical Link Control) - podvrstva logického řízení spoje zajišťuje přenos datových rámců na přenosové médium.
- **MAC** (Medium Access Control) - podvrstva řízení přístupu k médiu poskytuje rozhraní mezi fyzickou vrstvou a zařízením WI-FI (např. AP). A zároveň je zodpovědná za přenos dat.

Podvrstva MAC umožňuje několik způsobů režimu komunikace, který je řízen koordinačními funkcemi:

- **DCF** (Distributed coordination Function) - DCF funkce je základem standardního přístupového mechanismu CSMA/CA. Stejně jako Ethernet nejprve zkontroluje zda datové spojení je připraveno k použití před samotným přenosem. Aby se zabránilo kolizím, stanice používají náhodné odklady vysíláni (backoff) po každém přeneseném rámci. V některých případech může DCF použít naslouchací mechanismus CTS/RTS (Request To Send / Clear To Send) k dalšímu snížení možnosti kolizí.
- **CSMA/CA** (Carrier Sense Multiple Access with Collision Avoidance) - Všechny stanice před vysíláním poslouchají aktuální rádiový kanál. Pokud je detekován signál, médium je považován za obsazeno a stanice odloží své vysílání a čeká až bude přenosové médium volné. Tento systém používá pozitivní potvrzování. Zjednodušený princip CSMA/CA viz. příloha A.1.
- **RTS/CTS** - Mechanismus používá tzv. skrytého uzlu (stanice nejsou v vzájemném dosahu, neví o vysílání jiných stanic). Stanice vysílající paket si nastaví hodnotu NAV (virtuální naslouchání) a rezervuje si přenosové médium pro celou výměnu dat skládající se ze všech fragmentů paketu a ACK pro každý fragment.
- **PCF** (Point Coordination Function) - PCF funkce poskytuje služby contention-free (přístup k médiu bez boje). Aby stanice nemusely bojovat o médium jsou použity speciální stanice zvané bodové koordinátory (point coordinators). Tzv. point coordinators jsou umístěni v přístupových bodech, takže PCF je omezena na infrastrukturní sítě. PCF umožňuje stanicím vysílat rámce po kratším intervalu. Mechanismus PCF není příliš rozšířen a je určen pro synchronní datové přenosy pro sítě s přístupovými body.

1.7.1 MAC Frame Format [1]

Tato část popisuje 802.11 MAC formát rámce. Obecný MAC rámec (viz obr. 1.11) se skládá z několika částí:

- **Frame control** - Řídící rámec (viz. obr. 1.12) se skládá z několika částí:
  - Protocol Version - Dva bity, které obsahují informace o verzi protokolu.
  - Type a Subtype - Popisují typ použitého rámce: kontrolní rámce (Control frames), datové rámce (Data frames) nebo rámce pro správu (Management frames).
  - ToDS a FromDS - Tyto bity označují, zda rámec je určen pro distribuční systém.
  - More frag - Pokud byl „higher-level"paket fragmentován, počáteční fragment a všechny následující fragmenty se nastaví na log. 1.
  - Retry - Čas od času rámce mohou být přenášeny opakovaně. V případě, že rámec je opakovaně přenášen, pak tento bit je nastaven na hodnotu 1 (jinak 0). Pomáhá to přijímací stanici při odstraňování duplicitních rámců.
  - Power mgmt - Pokud je odesílající zařízení v úsporném režimu, pak tento bit je nastaven na 1 (jinak 0).

  - More data - Pokud je zařízení v režimu úspory energie, přístupový bod může uchovat rámce určené pro něj.
  - WEP - Pokud bylo použito šifrování těla rámce, pak se bit nastaví na 1.
  - Other - Nastavuje 1, pokud je povoleno striktní uspořádání rámců a fragmentů.

- **Duration/ID** - Určuje čas přenosu rámce a přijímaní ACK. Když je bit nastaven na 0, Duration/ID se používá k nastavení NAV . Hodnota představuje počet mikrosekund kdy médium zůstane zaneprázdněný přenosem. Všechny stanice musí sledovat záhlaví všech rámců, které dostávají, a podle toho aktualizují NAV.
- **Sequence control** - Je 12-bitová posloupnost čísel + 4 bitové číslo fragmentu. Slouží k eliminaci duplicitních rámců. Obsahuje číslo rámce a pořadí fragmentů.
- **Addresses** - Skupina adresních polí obsahuje 48-bitové adresy. Obsahují adresu zdroje (Source address), cíle (Destination address), přenašeče (Transmitter address), přijímače (Receiver address) a BSSID . Význam těchto adres závisí na tom, zda je rámec poslán do nebo z DS.
- **Frame body** - Tělo rámce, někdy nazýváno datové pole (Data field), obsahuje přenášená data. V 802,11 mohou přenášet rámce s maximálním užitečným zatížením 2304 bajtů dat.
- **FCS (Frame Check Sequence)** - Stejně jako u Ethernetu, 802.11 rámce uzavírá s kontrolním rámec sekvencí (FCS).FCS obsahuje kontrolní součet (CRC).

Obrázek 1.11: Obecný formát rámce

Obrázek 1.12: Frame control

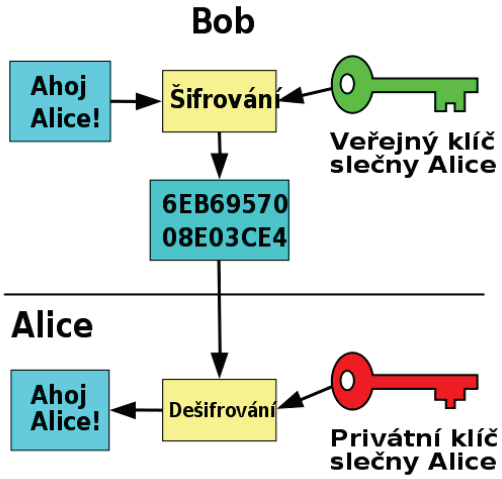
1.8 Šifrování [1]

Nezabezpečená síť je velmi riziková z hlediska útoků, a proto přenášené informace musí být šifrovány, aby se problému s útoky zamezilo. Jednotlivé šifrování můžeme rozdělit na:

- Symetrické šifrování - pro šifrování a dešifrování je použit stejný klíč. Typická šifra je DES.

- Asymetrické šifrování - pro šifrování a dešifrování se používají dva různé klíče: veřejný klíč (šifrování) a privátní klíč (dešifrování). Asymetrické šifrování má vyšší výpočetní náročnost a představitelem je např. RSA šifrování.

Obrázek 1.13: Příklad symterického šifrování [19]



Obrázek 1.14: Příklad asymterického šifrování [20]

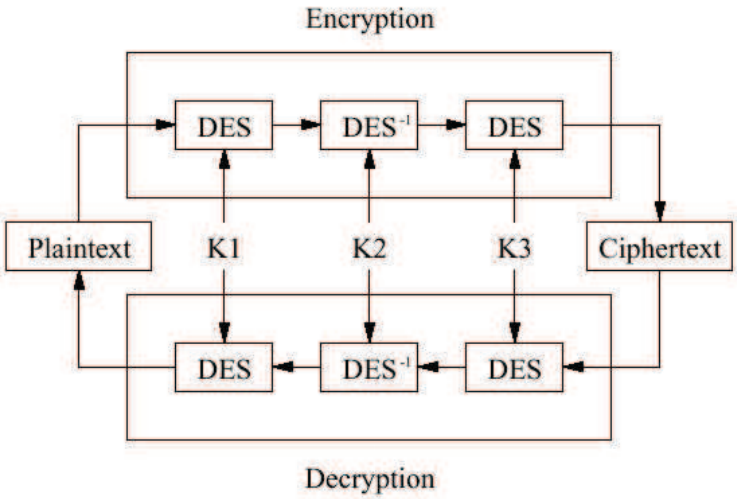
1.8.1 RC4

RC4 (Ron's Code 4) byl navržen Ronaldem Rivestem pro RSA Data Security v roce 1984. Je to bajtově orientovaná šifra. Každý byte z prostého textu je XORován s klíčovým bajtem čímž vznikne šifrovaný text. Vzhledem ke své jednoduchosti a rychlosti, je RC4 nejpoužívanější proudová šifra. Používá se v WEP zabezpečení pro šifrování a autentizaci.

1.8.2 DES a Triple-DES

Data Encryption Standard (DES) je symetrická šifra, kterou publikoval National Institution of Standards and Technology (NIST). DES je náchylná na brute-force útoky z důvodu omezené délky šifrovacího klíče (64-bitů). Její nejistá vnitřní struktura umožňuje National Security Agency (NSA) dešifrování zpráv bez šifrovacího klíče.

Triple-DES (DES kód třikrát opakuje) je určen k posílení DES. Využívá až tři 56-bitové klíče a umožňuje tři šifrování a dešifrování.



Obrázek 1.15: Princip Triple-DES

1.8.3 AES

Advanced Encryption Standard (AES) byl navržen jako nástupce DES a byl zveřejněn NIST v roce 2001. Jedná se o symetrickou blokovou šifru. Má pevnou velikost bloků 128 bitů a pracuje s klíči délky buď 128, 192, nebo 256 bitů. Větší klíčová velikost vede k vyššímu zabezpečení, ale taky k vetší náročnosti z hlediska výkonu. Tento standardizovaný algoritmus je použit ve WPA2.

1.9 Zabezpečení standardu IEEE 802.11 [22]

Bezdrátové sítě jsou založeny na rádiových vlnách, což dělá síťové médium náchylnějším k odposlechu. Tyto sítě musí být silně autentizovány, aby se zabránilo k přístupům neoprávněným uživatelům. Autentizované spojení musí být ochráněno šifrováním, aby se zabránilo k odposlechu či napadání provozu neoprávněnými stranami.

Zabezpečení dat je definován z hlediska tří atributů, z nichž všechny musí být zachovány pro zajištění bezpečnosti přenosu informací:

- **Integrity** - Jednoduše řečeno, integrita je ohrožena pokud jsou data modifikována neoprávněnými uživateli. („Změnil někdo neoprávněně data během přenosu?")
- **Secrecy** (utajení) - Posluchač na kanále datům nerozumí.
- **Availability** (dostupnost) - Informace musí být k dispozici, když je to potřeba. Nejčastější hrozbou jsou Denial-of-service útoky.

Nezabezpečená síť je pro uživatele velmi nebezpečná, protože přenášená data nejsou nějak chráněna šifrováním a do sítě se může připojit kdokoli, protože přístupový bod není zabezpečen.

1.9.1 SSID [5]

Každý přístupové bod (AP) v síti 802.11 pravidelně vysílá tzv. „beacon frame". Tyto rámce oznamují existenci sítě. Jsou použity v přístupových bodech, aby se jednotlivé stanice mohli najít a identifikovat síť. Každý „beacon frame"obsahuje Service Set Identifier (**SSID** zprávu), také často označenu jako název sítě, která jednoznačně identifikuje ESS (Extended Service Set).

Díky SSID se můžeme navázat spojení s AP. Parametr (klíč) SSID se skládá z řetězce ASCII znaků dlouhého maximálně 32 znaků. Vypnutím posílání SSID zpráv můžeme částečně zabezpečit síť.

1.9.2 MAC

Každé zařízení pracující v 802.11 sítích má přidělenou unikátní **MAC** (Media Access Control) adresu. Lze tak jednoduše zabezpečit provoz sítě tak, že na přístupových bodech se zapne MAC filtrace ve které se nastaví MAC adresy stanic, čímž dostanou stanice přistup do sítě. MAC adresy se dají klonovat, takže při její zjištění může kdokoli získat přistup do sítě.

1.9.3 WEP

Wired Equivalent Privacy (WEP) používá kryptografické metody pro ověřování a šifrování. Používá se symetrická šifra, takže pro šifrování i dešifrování používá stejné klíč. WEP zabezpečení v dnešní době není považováno za bezpečnou ochranu sítě. WEP používá proudovou šifru RC4 pro utajení a kontrolní součet CRC-32 pro integritu. Délka klíčů je 40, nebo 104 bitů + 24 bitů inicializačního vektoru.

Autentizace klienta může proběhnou dvěma způsoby: **Open key method** nebo **Shared key method**. Bez ohledu na použitou metodu, musí být stejná pro celý subsystém, tj zařízení a AP.

- **Open Authentication** - Otevřená autentizace dovoluje klientům se připojit na přístupový bod po odeslání identifikačních informací o klientu. Používá se pro sítě, které neprovádějí ověřování, stejně jako sítě, které jsou řešeny pomocí dynamického WEPu.
- **Shared Key Authentication** - Přístupový bod odešle paket s výzvou ke klientovi. Klient musí reagovat s textem šifrovaný pomocí správného klíče WEP. Některé systémy vyžadují MAC adresu které mají být použity s odpovědí, tak že na MAC adresu klienta musí odpovídat ten, který byl již dříve vstoupil do asociační tabulky přístupového bodu.

1.9.4 WEP+

WEPplus nebo WEP+ je proprietární rozšíření původního WEP zabezpečení společností Agere Systems. WEP+ se snaží odstranit slabé inicializační vektory („weak IVs"). Tyto slabé místa jsou snadno rozšifrovatelné (RC4) a může dojít k odposlechům v síti nebo k neoprávněném připojení do sítě.

1.9.5 WPA

Když se přišlo na nedostatky v WEP zabezpečení (původní 802.11 bezpečnostní standard), tak v roce 2003 WI-FI aliance přišla s novým zabezpečovacím protokolem WPA (Wi-Fi Protected Access). Je to dočasné řešení problémů WEP, WPA. Stále používá nezabezpečenou RC4 proudovou šifru, ale poskytuje další zabezpečení pomocí protokolu TKIP (Temporal Key Integrity Protocol). Pro autentizaci uživatelů používá standard 802.1x.

Poznámka 1.2 TKIP protokol využívá stávající hardware WEP, na kterém běží šifrování RC4 a snaží se chránit generované klíče, které jsou zranitelné. TKIP je skutečná obálka pro WEP a funguje na základě jednotlivých paketů.

1.9.6 WPA2 (IEEE 802.11i)

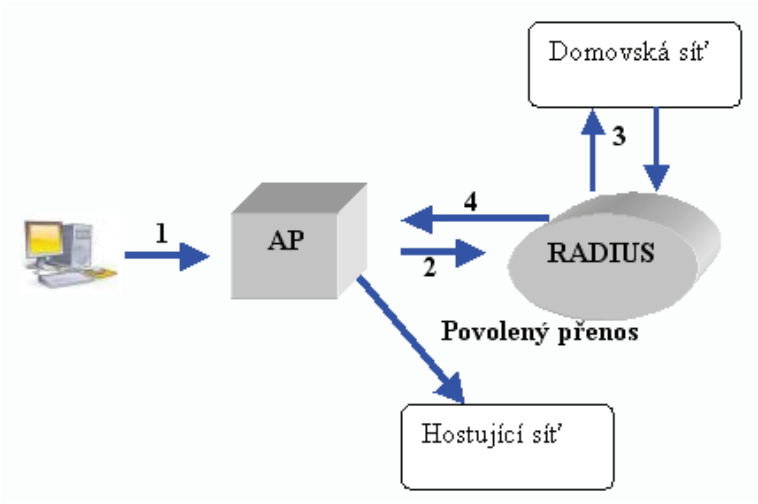
Kvůli slabému zabezpečení WEP a WPA v roce 2004 vyvinula vyvinula WI-FI aliance bezpečnostní protokol WPA2. Na rozdíl od WEP a WPA, WPA2 používá blokovou šifru AES (Advanced Encryption Standard) namísto RC4 proudové šifry. CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) nahrazuje TKIP.

Pro zabezpečení dat využívá následující komponenty. 802.1x pro autentizaci (s využitím EAP a autentizačního serveru), RSN (Robust Security Network) pro udržování záznamů asociací a na AES založený CCMP jenž se stará o šifrování dat.

1.9.7 802.1x [21]

Protokol definuje obecný bezpečnostní rámec pro všechny druhy sítí. Zajišťuje autentizaci uživatelů, distribuci klíčů a šifrování (integritu zpráv). Pro autentizaci je používán na straně klienta program tzv. suplikant (prosebník), jemuž AP umožní komunikaci s třetí stranou, která ověření provede např. RADIUS server.

Struktura protokolu: „klient - přístupový bod - autorizační server RADIUS".



Obrázek 1.16: Princip 802.11x

1.9.8 Směrové antény

Další způsobem jak částečně zabezpečit síť je použitím směrových antén. Pokud se přijímače např. počítače nachází v jednom směru od přístupového bodu, tak lze použít směrovou anténu. V případě narušení provozu sítě, by musel být útočník ve směru antény.

	Autentizace	**Šifrování**	**Vhodné pro firemní sítě WAN**	**Vhodné pro domácnosti a malé firmy sítě WLAN**
WEP	-	WEP	slabé	méně než dobré
WPA (PSK)	PSK	TKIP	slabé	nejlepší
WPA (PSK)	PSK	AES-CCMP	slabé	nejlepší
WPA	802.1x	TKIP	lepší	dobré (nákladnější)
WPA 2	802.1x	AES-CCMP	nejlepší	dobré (nákladnější)

Tabulka 1.3: Porovnání zabezpečení [18]

2 Postup měření bezdrátových sítí

Měření probíhalo pomocí bezdrátového USB adaptéru TP-LINK TL-WN722N, který byl připojen v notebooku a měřilo se v budovách s několika dostupnými přístupovými body. Následně byly použity open-source nástroje pro analýzu a monitoring sítí (viz. kap. 3).

2.1 Popis TP-LINK TL-WN722N [16]

Pro měření byl použit bezdrátový USB adaptér TL-WN722N s odjímatelnou všesměrovou anténou 4 dBi. Karta podporuje standardy IEEE 802.11n/b/g a její maximální přenosová rychlost je 150 Mbit/s.

Max. přenosová rychlost	150 Mbit/s
Rozhraní	USB 2.0
Typ antény	Odnímatelná všesměrová
Zisk antény	4 dBi
Podporované standardy	IEEE 802.11n, IEEE 802.11g, IEEE 802.11b
Frekvence	2,400–2,4835 GHz
Modulační technologie	DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM
Zabezpečení bezdrátové sítě	Podpora šifrování 64/128 bit WEP, WPA-PSK/WPA2-PSK, filtrování MAC
Bezdrátové režimy	Režim Ad-Hoc/infrastruktury
EIRP	max. 20 dBm

Tabulka 2.1: Specifikace bezdrátové karty TP-Link TL-WN722N

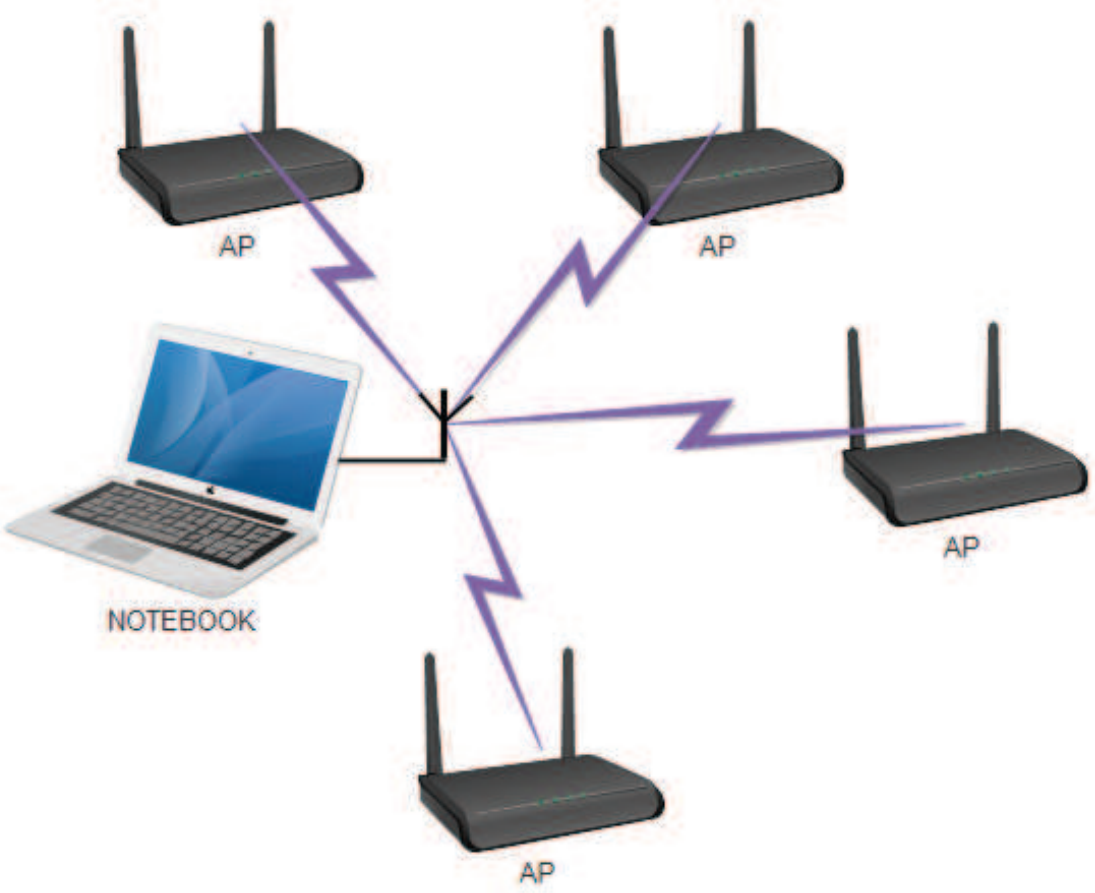
Obrázek 2.1: Bezdrátová karta TP-Link TL-WN722N

2.2 Schéma zapojení

Pro měření bylo použito jednoduché zapojení, které se skládá z následujících komponent:

- **Notebook (PC)**
- **Bezdrátová karta**
- **Přístupové body (AP)**

K notebooku byla připojena bezdrátová karta do USB portu a pak se použily nástroje pro analýzu a sledování provozu sítě, které zachycují veškerý datový provoz jednotlivých přístupových bodů. Testovací topologií je infrastrukturální síť.



Obrázek 2.2: Schéma zapojení

2.3 Testování nástrojů

Každý vybraný nástroj je otestován z hlediska možnosti sledování a analýzy bezdrátových sítí. U nástrojů byl kladen důraz na:

- zobrazení základních parametrů sítě,
- zachytávání paketů,
- možnost užití paketového filtru,
- možnosti analýzy,
- sledování vytížení sítě a kanálů,
- možnosti zobrazení grafů,
- export do souboru,
- podporu operačního systému,
- ovládání pomocí příkazového řádku nebo grafického rozhraní,
- uživatelskou náročnost,
- přehlednost.

Popis a možnosti nástrojů jsou popsány v kapitole 3 a v kapitole 5 jsou pak nástroje porovnány v programem KISMET.

3 Nástroje pro monitoring a analýzu bezdrátových sítí

V dnešní době existuje několik milionů fungujících WIFI sítí v domácnostech, na veřejnosti, ve firmách no prostě všude kde se dá. Kvůli takovému počtu těchto sítí a kvůli bezpečnosti je sítě potřeba monitorovat a analyzovat. Proces monitorování a analyzování umožňuje sledovat a mapovat bezdrátové sítě a může taky sloužit jako upozornění např. špatného nastavení sítě. V České republice jsou bezdrátové sítě hlídané ČTU (Český telekomunikační úřad).

Existuje spousta programů pro tento účel jak placené či neplacené. Tato práce je zaměřena na open-source programy.

Základní způsob monitoringu a analýzy bezdrátových sítí lze provést pomocí jednoduchých příkazů v příkazovém řádku např. pomocí nástroje netsh (MS Windows viz. kap. 3.2.1) a nebo pomocí programů ovládané přes GUI nebo konzoli např. Kismet (viz. kap. 3.1.2).

3.1 Open-source nástroje bežící na Linux platformě

3.1.1 iwlist a nm-tool [12]

Nejsnadnější způsob jak získat základní informace o sítích je použití jednoduchých příkazů nebo balíčků například iwlist nebo nm-tool.

3.1.1.1 nm-tool Nástroj nm-tool poskytuje informace o síťovém manažeru (NetworkManager), zařízení a bezdrátových sítí. Jednoduchým příkazem lze získat požadované informace o dostupných sítích:

```
nm-tool | grep "Freq.*Strength" | sed -ne "s|\(.*Strength\ \([0-9]\+\).*\)|\2}\1|
p" | sort -n -r
```

Výpis 1: Ukázka příkazu nm-tool nástroje

```
73}    Wifi-Network:    Infra, F8:1A:67:41:27:10, Freq 2462 MHz, Rate 54 Mb/s, Strength 73 WPA WPA2
72}    *Wifi-Network:   Infra, F8:1A:67:41:27:10, Freq 2462 MHz, Rate 54 Mb/s, Strength 72 WPA WPA2
49}    TP-LINK_E883F4:  Infra, 00:21:27:E8:83:F4, Freq 2437 MHz, Rate 54 Mb/s, Strength 49
39}    TP-LINK_E883F4:  Infra, 00:21:27:E8:83:F4, Freq 2437 MHz, Rate 54 Mb/s, Strength 39
20}    mananex:         Infra, 14:D6:4D:7D:0D:36, Freq 2437 MHz, Rate 54 Mb/s, Strength 20 WPA WPA2
15}    dornak:          Infra, 04:8D:38:4B:C0:23, Freq 2412 MHz, Rate 54 Mb/s, Strength 15 WPA WPA2
9}   slfree_snehurka_2: Infra, 00:0B:6B:35:D1:D5, Freq 2472 MHz, Rate 11 Mb/s, Strength 9
```

Obrázek 3.1: Ukázka výpisu informací po použití nástroje nm-tool

3.1.1.2 iwlist Příkaz iwlist umožňuje získat základní informace o dostupných přístupových bodech. Následujícím příkazem lze získat informace o sítích:

```
sudo iwlist wlan1 scanning | egrep 'Cell |Rate|Frequency|
Encryption|Quality|Last beacon|ESSID'
```

Výpis 2: Ukázka použití příkazu iwlist

```
Cell 01 - Address: F8:1A:67:41:27:10
          Frequency:2.462 GHz (Channel 11)
          Quality=60/70  Signal level=-50 dBm
          Encryption key:on
          ESSID:"Wifi-Network"
          Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s; 6 Mb/s
          Bit Rates:24 Mb/s; 36 Mb/s; 48 Mb/s; 54 Mb/s
          Extra: Last beacon: 324ms ago
Cell 02 - Address: 00:21:27:E8:83:F4
          Frequency:2.437 GHz (Channel 6)
          Quality=33/70  Signal level=-77 dBm
          Encryption key:off
          ESSID:"TP-LINK_E883F4"
          Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s; 6 Mb/s
          Bit Rates:9 Mb/s; 18 Mb/s; 48 Mb/s; 54 Mb/s
          Extra: Last beacon: 4304ms ago
```

Obrázek 3.2: Ukázka výpisu informací po použití příkazu iwlist

3.1.2 Kismet [15]

Kismet je 802.11 detektor sítě, sniffer a intrusion detekční systém. Kismet bude pracovat pouze s bezdrátovou kartou, která podporuje monitorovací režim. Může analyzovat protokoly 802.11b, 802.11a, 802.11g a 802.11n provoz (zařízení, které to dovolují).

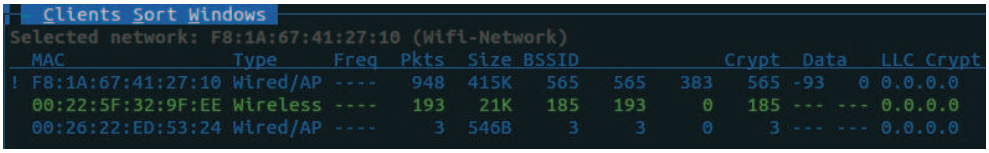
Kismet identifikuje sítě prostřednictvím pasivního sběru paketů, což umožňuje detekovat skryté sítě a přítomnost „non-beaconing"sítí.

Obrázek 3.3: Kismet

Úvodní obrazovka obsahuje seznam dostupných přístupových bodů a jejich nastavení - název sítě, počet přijatých paketů, kanál a typ sítě atd.

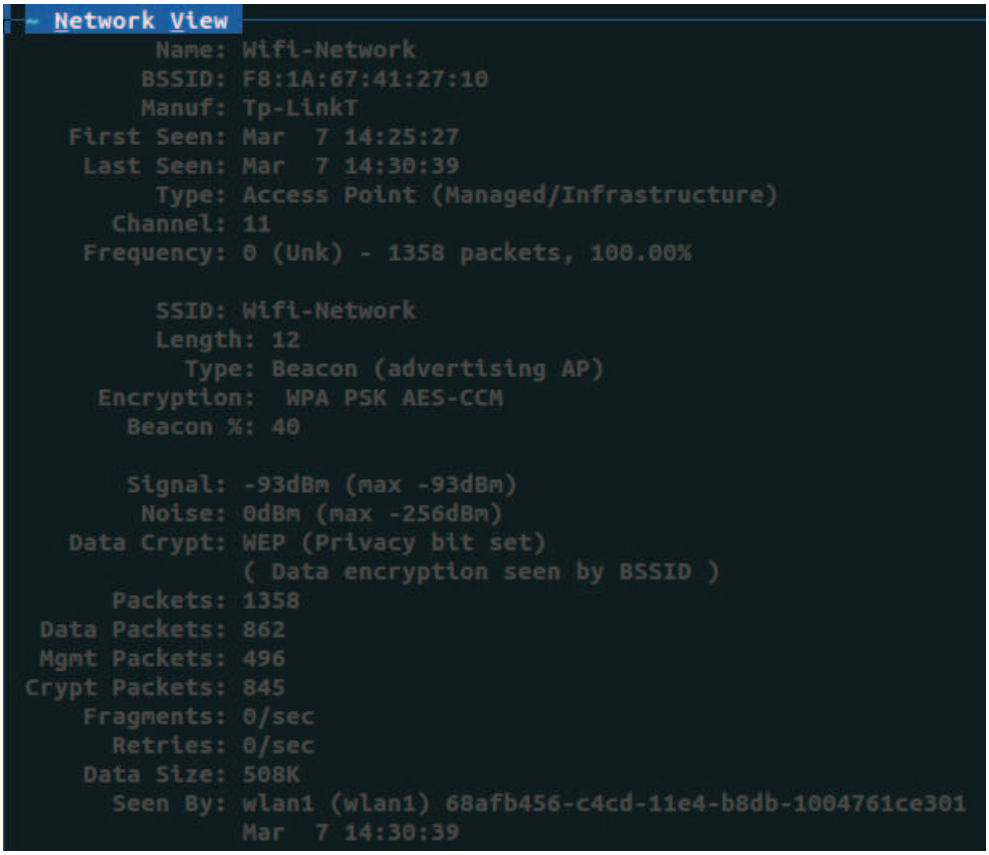
Ve spodní část můžeme najít tzv. stavové informace (např. nově detekovaná síť), graf počtu zachycených paketů a zobrazení klientů připojených na jednotlivých sítích.

Na pravé straně obrazovky se nachází informace o celkovém běhu aplikace, počet detekovaných sítí, počet zachycených paketů, průtok dat za sekundu nebo filtrované pakety (viz. obr.3.3).

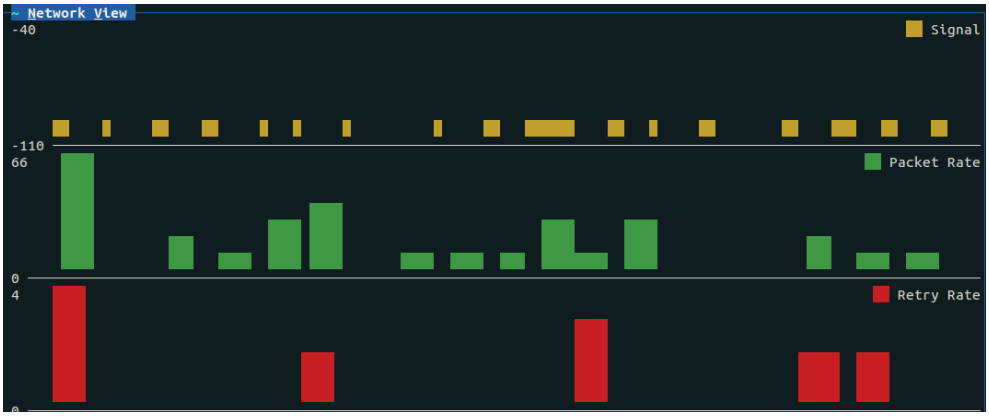


Obrázek 3.4: Kismet - zobrazení klientů připojených na zvolené síti

Kismet dále umožňuje zobrazit detailní informace o zvolené síti (viz. obr. 3.5), grafické znázornění pomocí grafů (viz. obr. 3.6) a nebo zobrazení klientů na síti (viz. obr. 3.4).



Obrázek 3.5: Kismet - detailní informace o síti



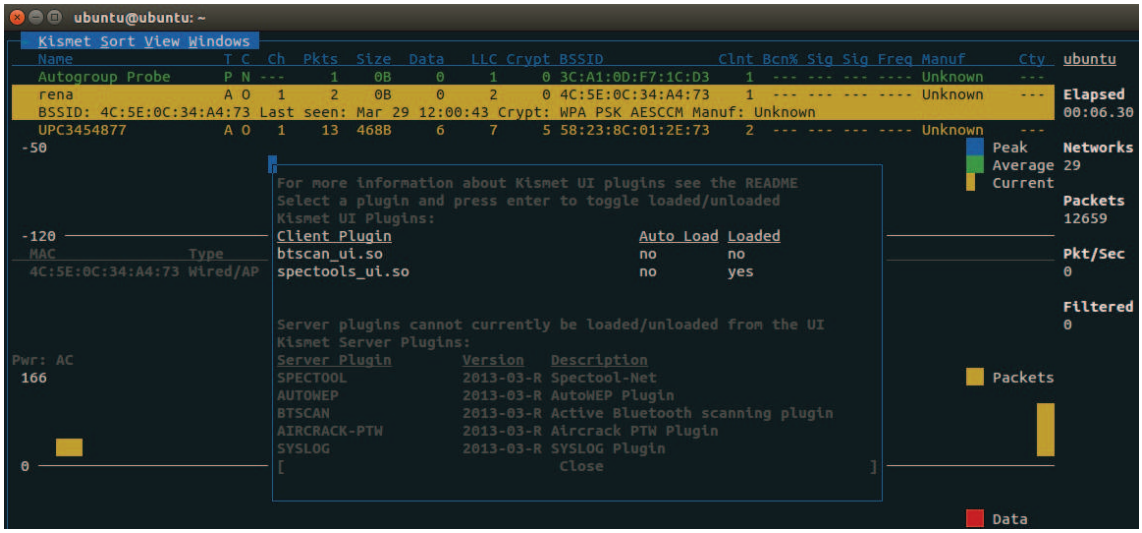
Obrázek 3.6: Kismet - zobrazení grafů sítě (signal, packet rate, reply rate)

Kismet podporuje instalace různých pluginů pro práci z bezdrátovými sítěmi, které rozšiřují možnosti samotného programu. Základní pluginy do nástroje lze získat následujícím příkazem:

```
sudo apt-get install kismet-plugins
```

Výpis 3: Kismet - instalace základních pluginů

Pro provedení příkazu se zobrazí v Kismetu možnosti volby různých pluginů, které se nainstalovaly. Jako užitečný plugin lze považovat „spectools", který nám umožní zobrazit spektrum signálů bezdrátových sítí (viz. obr. 3.7).



Obrázek 3.7: Kismet - aktivace pluginů

Kismet nepodporuje jen vlastní pluginy, ale podporuje možnost rozšířit nástroj pluginy z různých balíčků např. Aircrack.

Nástroj zaznamenává zachycené data do souboru. Soubory lze pak otevřít např. ve Wiresharku, kde se lze podívat detailně na zachycený provoz a provést analýzu.

3.1.3 Aircrack-ng [9]

Aircrack-ng je soubor balíčků, které umožňují analýzu bezdrátových sítí 802.11, „sniffe-rování"paketů, testování zabezpečení sítě a nebo se často používá k prolomení hesel wifi sítí, které používají zabezpečení WPA nebo WPA-PSK. Nástroj potřebuje k chodu bez-drátovou kartu s monitorovacím režimem. Aircrack-ng je konzolová aplikace a ovládá se pomocí jednoduchých příkazů.

Jak už bylo zmíněno balíček **aircrack-ng** obsahuje mnoho funkcí například:

- **aircrack-ng** - Slouží k prolamování hesel
- **airmon-ng** - Slouží k přepínaní wifi karty do monitorovacího režimu
- **aireplay-ng** - Injekce paketů
- **airodump-ng** - Packet sniffer: zobrazuje informace o sítích.

a spoustu dalších možností práce se sítí. Jak už bylo zmíněno balíček **airodump-ng** slouží k získaní informací o sítích viz. následující příkaz:

```
airodump-ng wlan1
```

Výpis 4: Příklad užití balíčku airodump-ng

```
CH 10 ][ Elapsed: 4 mins ][ 2015-03-07 15:06

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

F8:1A:67:41:27:10  -57      315      595    0  11  54e. WPA2 CCMP   PSK  Wifi-Net
14:D6:4D:7D:0D:36  -84       98        0    0   6  54e  WPA2 CCMP   PSK  mananex
00:0B:6B:35:D1:D5  -90       48        2    0  13  11 . OPN              slfree_s
04:8D:38:4B:C0:23  -90       29        0    0   1  54e  WPA2 CCMP   PSK  dornak

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   10:08:C1:98:4A:25  -90    0 - 1      0         6  wifi_nika
F8:1A:67:41:27:10  70:1A:04:7D:EA:06  -37    0 -48      0         6
F8:1A:67:41:27:10  00:22:5F:32:9F:EE  -62   54e-54e   116       584  Wifi-Network
00:0B:6B:35:D1:D5  00:02:72:62:64:D2   -1   11 - 0      0         1
```

Obrázek 3.8: Výpis z programu po použití balíčku airodump-ng

Airodump-ng detekuje dostupné sítě a připojené klienty. Umožňuje taky zobrazit základní údaje sítě např. typ šifrovaní, úroveň signálu, atd. (viz. obr. 3.8).

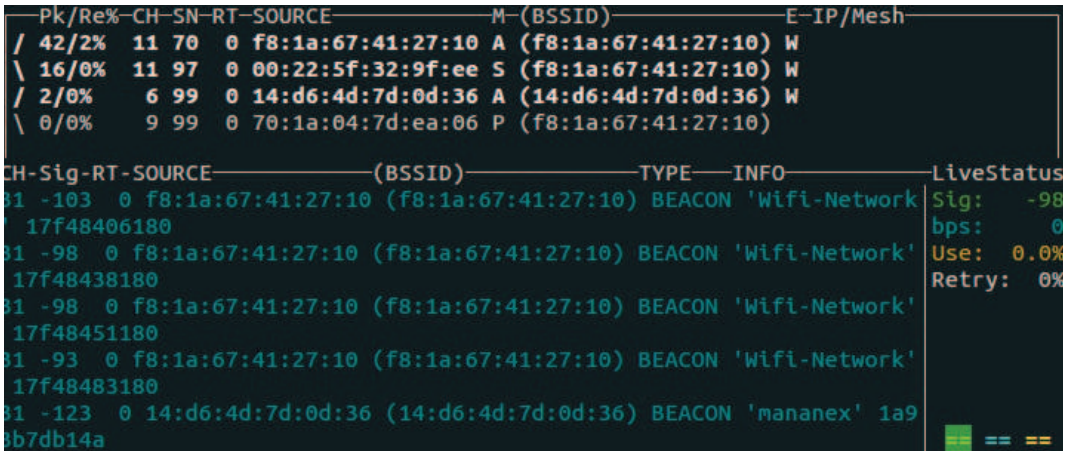
3.1.4 Highly Optimized Radio Scanning Tool [10][11]

Highly Optimized Radio Scanning Tool nebo-li horst je lehký IEEE 802.11 analyzátor pro bezdrátové sítě s textovým rozhraním. Jeho základní funkce jsou podobné nástrojům tcpdump, Wireshark nebo Kismet, ale je to mnohem menší nástroj a ukazuje různé souhrnné informace o síti, které nejsou snadno dostupné z jiných podobných nástrojů nástrojů. Nástroj je zaměřen především na ladění bezdrátové sítě se zaměřením na mód ad-hoc (IBSS). Horst nám umožňuje získat rychlý přehled o tom, co se děje na všech bezdrátových kanálech a případně zjistit problémy.

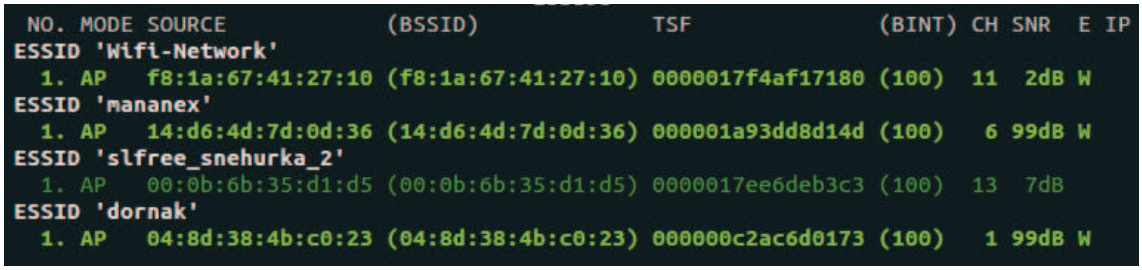
Opět je tu nutnost, aby příslušná bezdrátová karta podporovala monitorovací režim.

3.1.4.1 Funkce

- Ukazuje úroveň signálu/šumu každé stanice
- Počítá využití kanálu sečtení času paketů, které používají(zabírají) médium.
- „Spektrum Analyzer"ukazuje úroveň signálu a využití každého kanálu.
- Grafické zobrazení historie paketů, typu paketů nebo fyzické rychlosti.
- Zobrazí všechny stanice podle ESSID a TSF každého uzlu.
- Detekuje IBSS „splits"(stejné ESSID, ale jiný BSSID - to je běžný problém ovladače)
- Statistiky paketů/ bytů podle fyzické rychlosti a podle typu paketů.
- Lze filtrovat specifické pakety podle zdrojové adresy nebo BSSID.
- Podpora klienta/serveru pro sledování provozu na vzdálených uzlech.

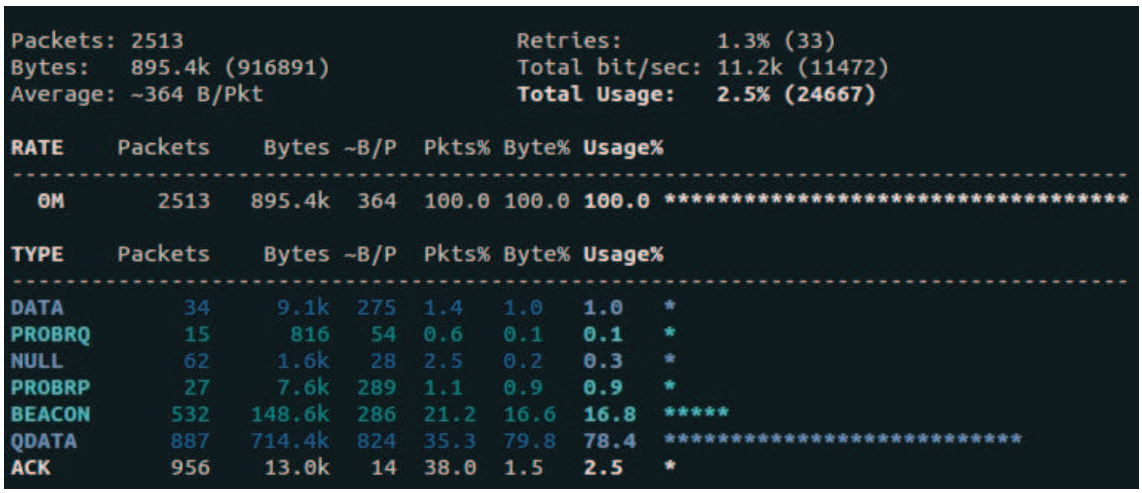


Obrázek 3.9: horst - Hlavní okno: Přehled zachycených paketů, zobrazení seznamu aktivních uzlů a jejich SNR. Zobrazuje také bar s uvedením, jak využíván je kanál



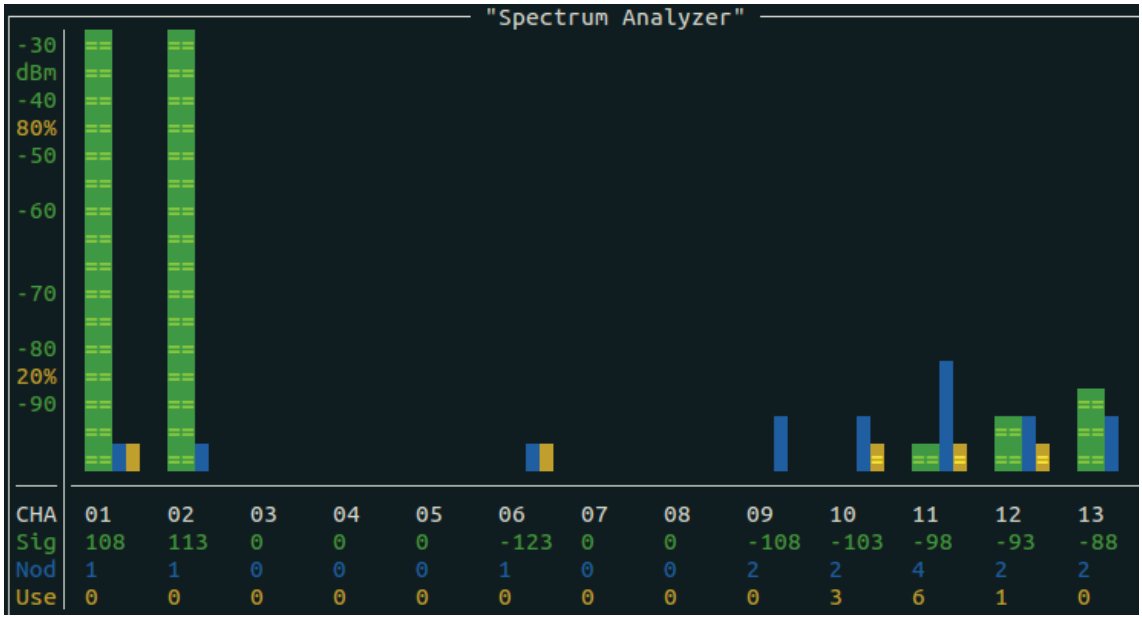
Obrázek 3.10: horst - Přehled zachycených přístupových bodů

Obrázek 3.11: horst - Přehled historie Signal/Noise/Rate

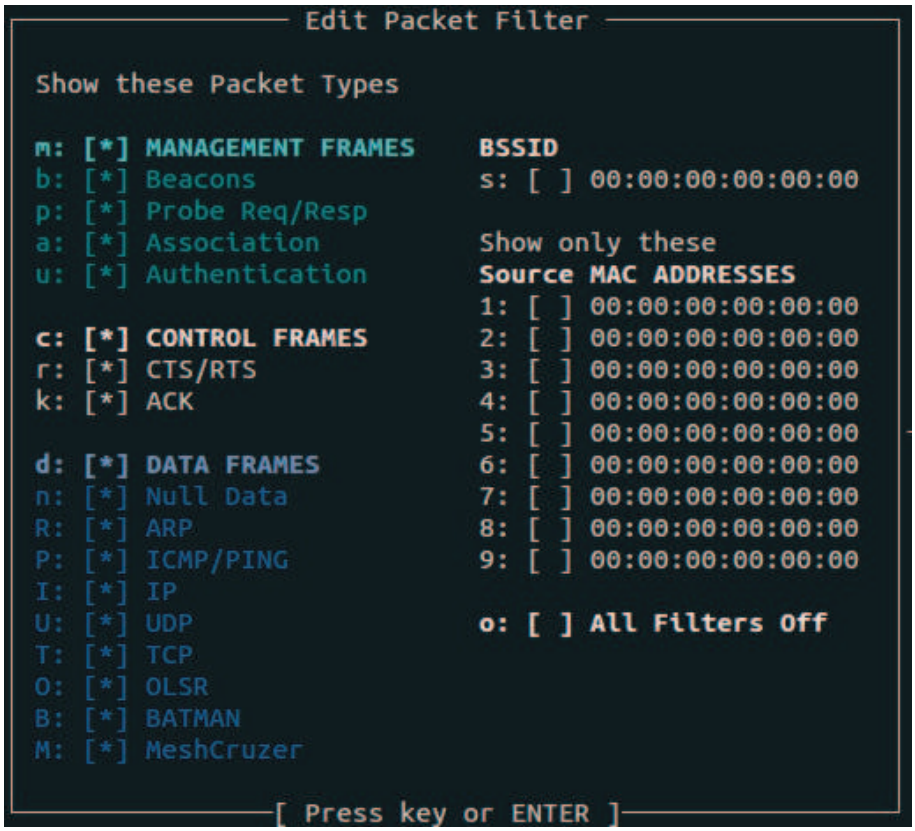


Obrázek 3.12: horst - Statistiky paketů

Highly Optimized Radio Scanning Tool taky umožňuje filtrovat zachycené pakety, což umožňuje lepší práci s nástrojem např. pokud chceme zjistit přesné údaje o paketech a přebytečné informace jsou filtrem nezobrazovány (viz. obr. 3.14).



Obrázek 3.13: horst - Spectrum Analyzer

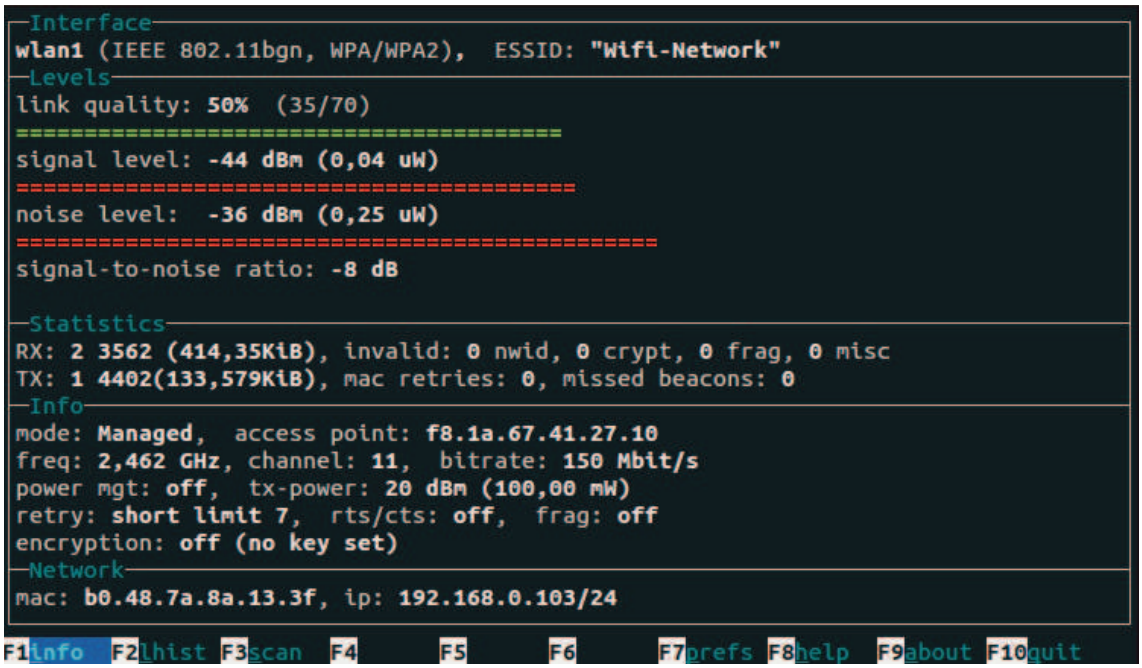


Obrázek 3.14: horst - paketový filtr

3.1.5 Wavemon [13]

Wavemon je založený na ncurses knihovnách a je určen pro monitorování bezdrátových zařízení. Umožňuje sledovat signál a hladinu šumu, statistiky paketů, konfiguraci zařízení, a parametry síťového hardwaru bezdrátových sítí.

Wavemon původně vyvinul Jan Morgenstern.



Obrázek 3.15: Wavemon

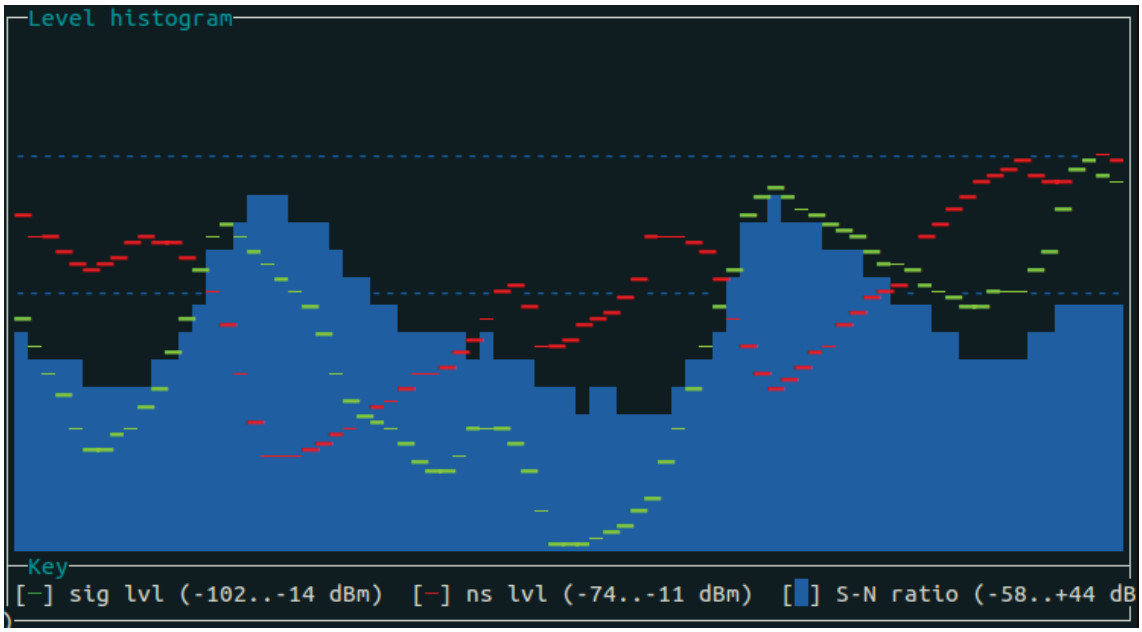
Rozhraní Wavemonu je rozděleno na několik „obrazovek"například úvodní obrazovka zobrazuje základní informace o bezdrátové sítí.

3.1.5.1 Rozdělení a funkce programu

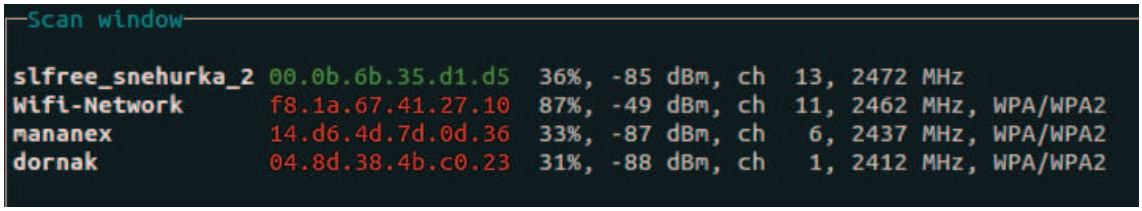
- **Info (F1)** - Zobrazuje zhuštěný přehled všech dostupných bezdrátových specifických parametrů a statistických údaje údajů o síti. Taky jsou zobrazeny grafy aktuálního signálu a kvality linky (viz. obr. 3.15). Obrazovka se dále dělí na subsekce:
  - **Interface** - Zobrazuje používané rozhraní (např. wlan0) a ESSID sítě, na kterou je připojeno rozhraní.
  - **Levels** - Tato část zobrazuje grafy aktuálního signálu, šumu nebo kvality linky.
  - **Statistics** - Tato sekce zobrazuje čítače odeslaných/přijímaných paketů a bajtů. Zobrazuje taky počet paketů, které byly zahozeny rozhraním z důvodu neplatných ID sítě, nesprávných šifrovacích klíčů a jiných chyb.
  - **Info** - Subsekce „Info"zobrazuje aktuální stav používaného rozhraní. Lze vyčíst nastavení režimu rozhraní, šifrování, úroveň výkonu a mnoho další.

  - **Network** - Poslední sekce zobrazuje např. MAC adresu nebo broadcast adresu sítě.

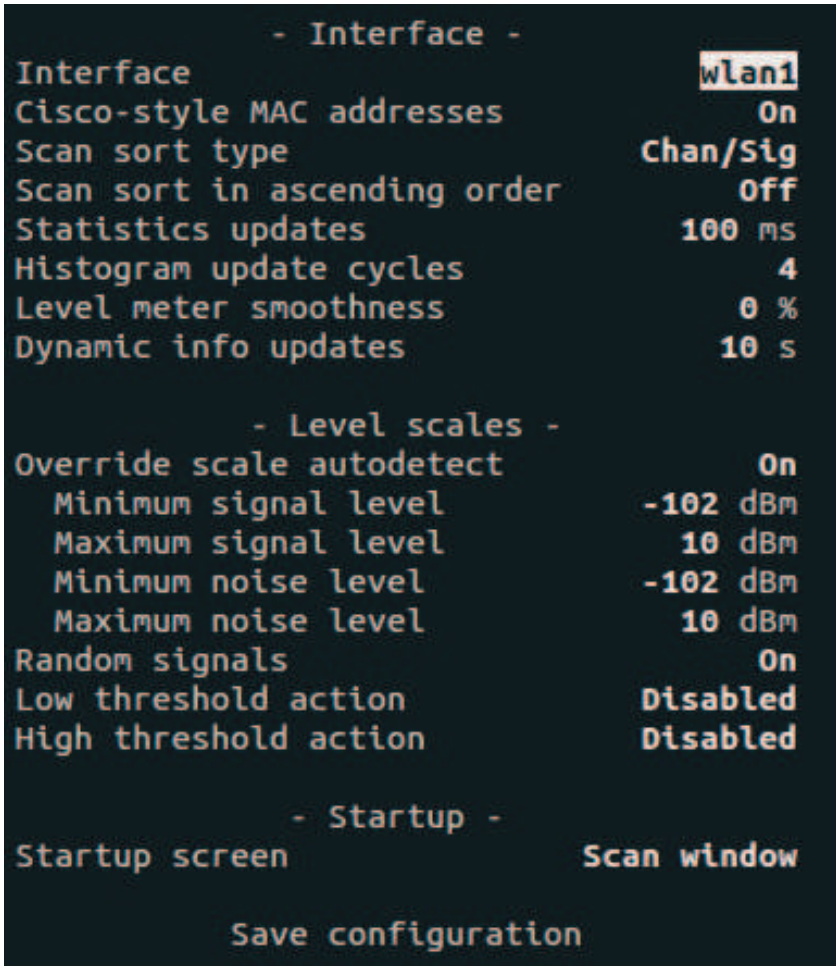
- **Level histogram (F2)** - Tato část programu zobrazuje grafy signálových úrovní, úrovní šumu nebo úrovní signal-to-noise (viz. obr. 3.16).
- **Access point list (F3)** - Tato obrazovka obsahuje seznam dostupných přístupových bodů v okolí a jejich základní informace např. sílu signálu, MAC adresu (viz. obr. 3.17).
- **Preferences (F7)** - V této sekci se nachází nastavení programu. Můžeme zde nastavit interface, který bude wavemon používat, nastavení grafů (měřítka) atd. (viz. obr. 3.18).
- **Help (F8)** - Sekce s nápovědou.
- **About (F9)** - Informace o programu.
- **Quit (F10)** - Ukončení programu.



Obrázek 3.16: Wavemon - Ukázka výstupních grafů - úroveň signálu, šumu, S-N ratio



Obrázek 3.17: Wavemon - Ukázka výpisu dostupných přístupových bodů



Obrázek 3.18: Wavemon - Možnosti nastavení programu

3.1.6 Wireshark [26]

Wireshark je nejrozšířenější protokolový analyzátor (dříve Ethereal). Zachytává informace o veškerém provozu mezí rozhraními. Na základě těchto informací lze provést analýzu a získat podrobné informace např. o chybách sítě nebo odhalení špatného směrování v síti. Nástrojem se lze podívat na IEEE 802.11 hlavičku a zobrazit si detailní informace o částech rámce.

Nástroj je vydáván na různých platformách:

- Linux
- MAC OS
- Microsoft Windows
- Solaris, BSD

a je kompatibilní z většinou nástrojů umožňující zachytávat síťovou komunikaci. Provoz lze zachytávat z různých rozhraní:

- Ethernet
- IEEE 802.11
- Bluetooth
- USB

a spoustu dalších. Wireshark dále nabízí hloubkovou analýzu programů a dešifrování různých protokolů. Podporuje aplikaci různých pluginů a export do souboru (CSV, XML, textový soubor).

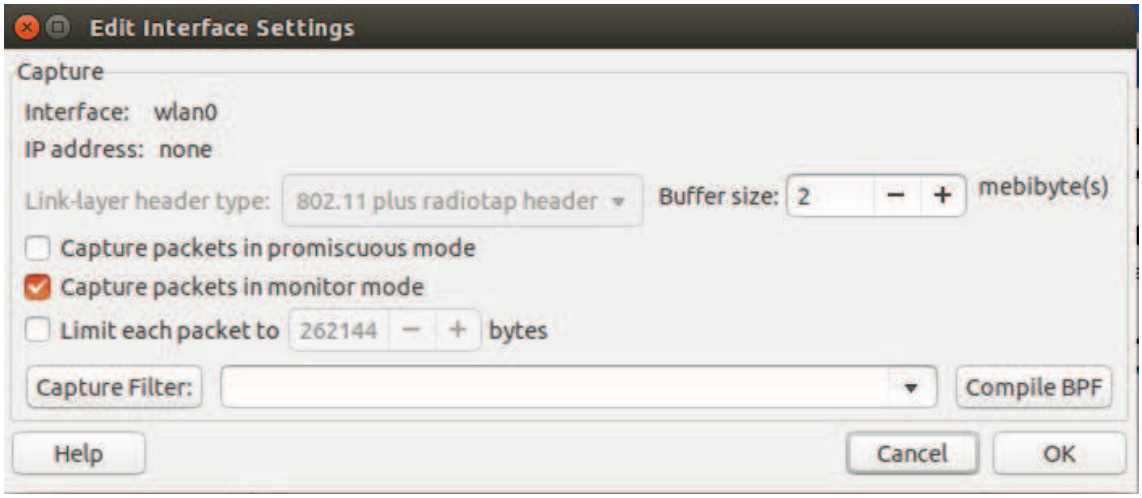
Následující obrázek 3.19 ukazuje nastavení rozhraní, kde Wireshark zachycuje pakety v monitorovacím režimu.

Wiresharkem můžeme získat základní údaje (např. signál, typ sítě, frekvence, rate) o síti viz obr. 3.20. Samotný nástroj umožňuje získat opravdu detailní informace o provozu sítě:

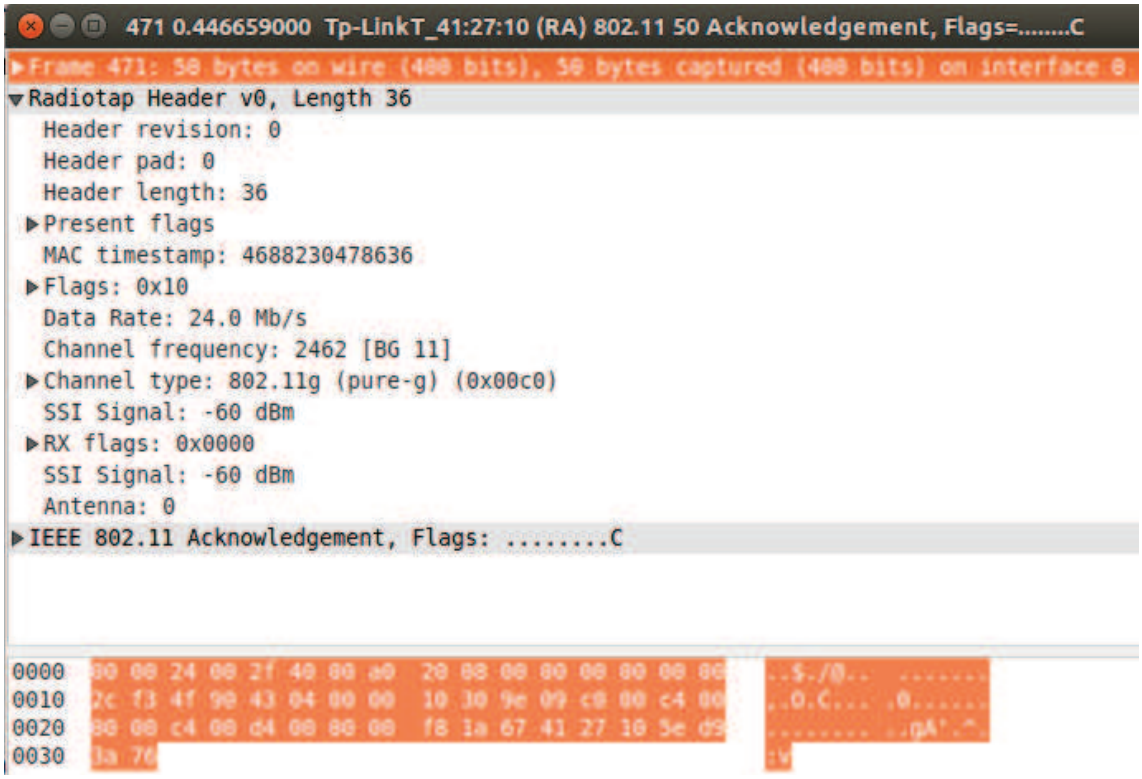
- o paketech,
- o zachycených rámcích,
- o protokolech,
- o klientech

viz. obrázek 3.21. Dále je možné tyto údaje filtrovat a zobrazit je v celkových statistikách ze kterých se provede následná analýza.

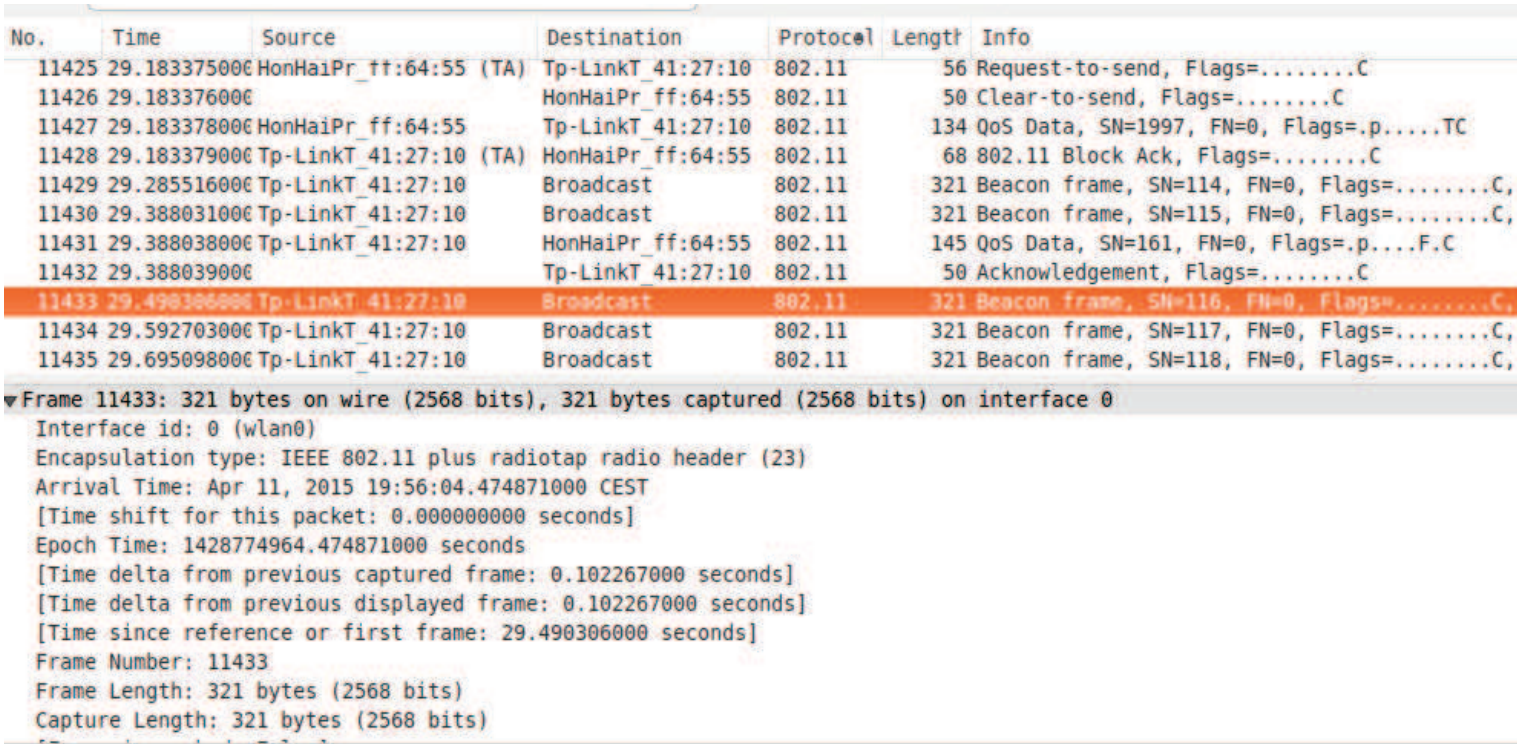
Veškeré informace jsou zobrazeny pomocí GUI. Wireshark existuje i v konzolové aplikaci tzv. TShark, který lze ovládat pomocí příkazu v terminálu.



Obrázek 3.19: Wireshark - Nastavení rozhraní



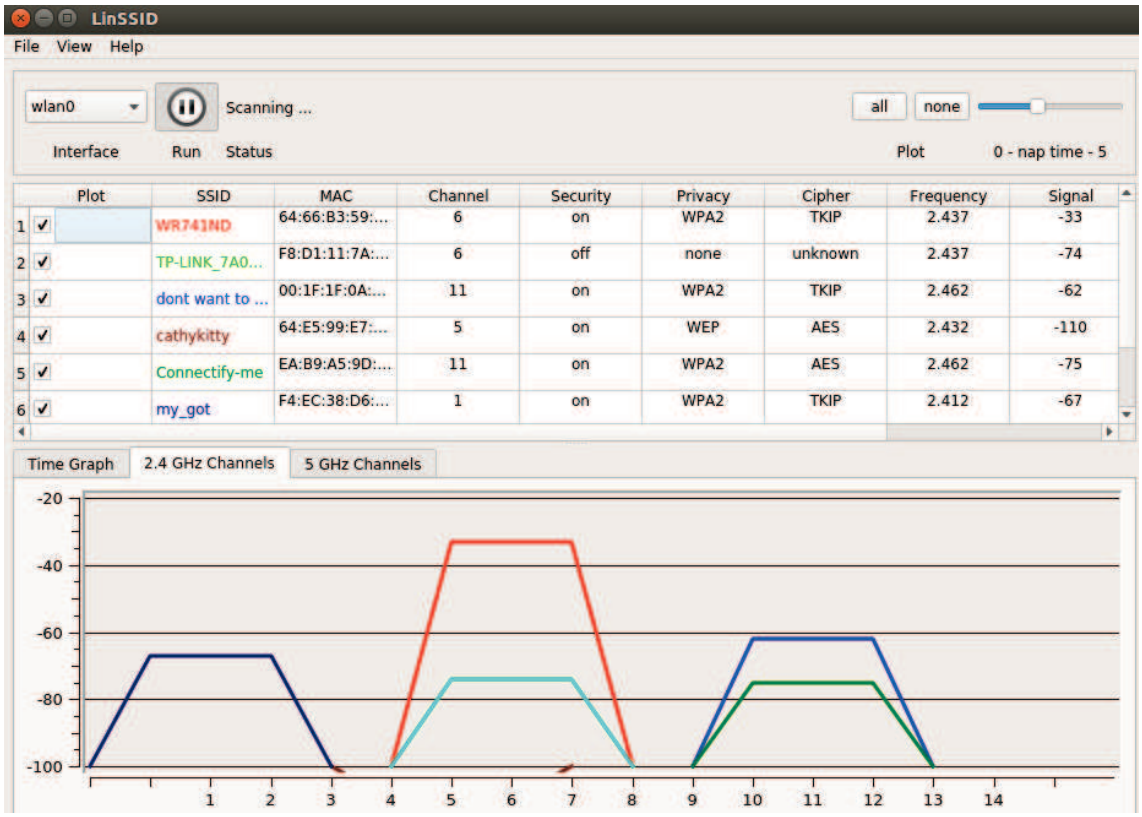
Obrázek 3.20: Wireshark - Informace o síti



Obrázek 3.21: Wireshark - Detailní informace o provozu sítě

3.1.7 LinSSID [23]

LinSSID grafický linuxový program umožňuje monitorování bezdrátových sítí. Je graficky i funkčně podobný InSSIDer (Microsoft Windows® ™). Je napsán v C ++ s použitím bezdrátových nástrojů Linuxu, Qt5 a Qwt 6.1.



Obrázek 3.22: LinSSID

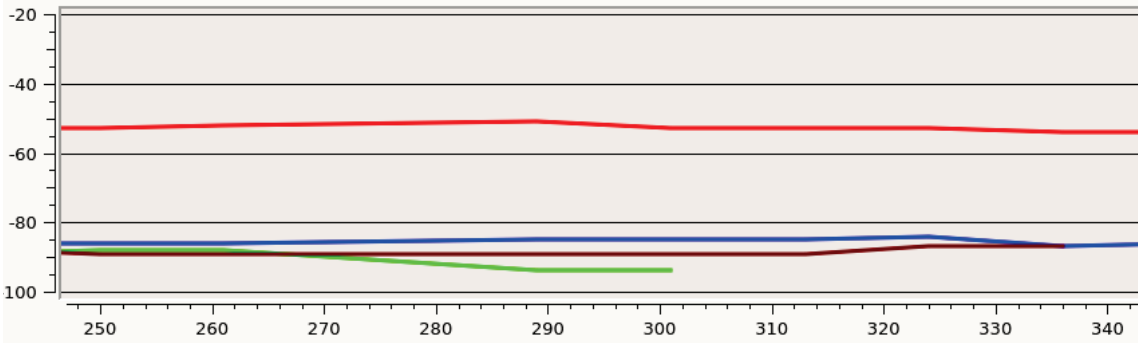
3.1.7.1 Funkce programu

Možnosti programu se velmi podobají programu InSSIder (viz. kap. 3.2.2). Oproti již zmíněném programu nabízí více informací o dostupných sítí např.:

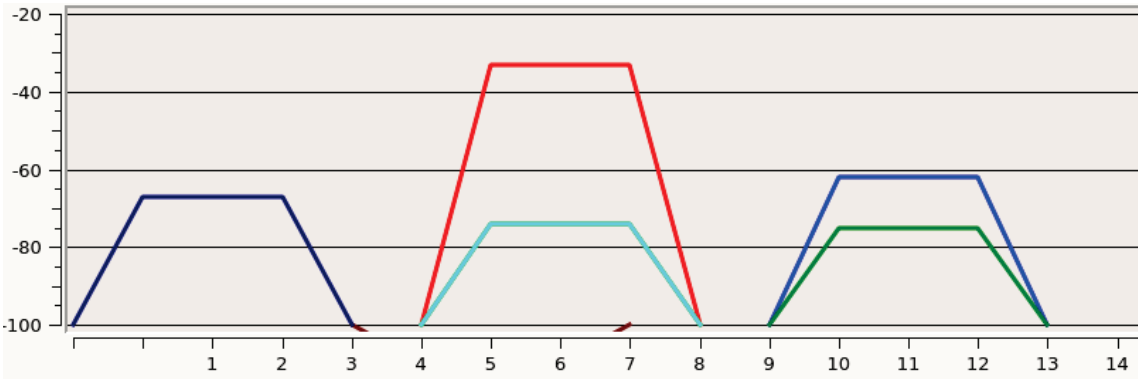
- **Min Sig** - maximální úroveň signálu
- **Max Sig** - minimální úroveň signálu
- **Noise** - šum
- **Protocol** - používaný protokol
- **Qualitity** - kvalita linky

- **Cipher** - šifrování
- **Mode** - mód rozhraní např. Master

Stejně jako InSSIDer umožňuje zobrazovat jednotlivé grafy, které zobrazují sílu přijímaného signálu v čase (viz. obr. 3.23) a nebo zobrazují bezdrátové sítě s použitými kanály, což může odhalit špatné nastavení kanálů a odhalit např. zdroj rušení (viz. obr. 3.24).



Obrázek 3.23: LinSSID - Úrovně přijímaných signálů bezdrátovou kartou



Obrázek 3.24: LinSSID - Zobrazení jednotlivých kanálů používané sítěmi

3.2 Open-source nástroje bežící na MS Windows platformě

3.2.1 Network shell [14]

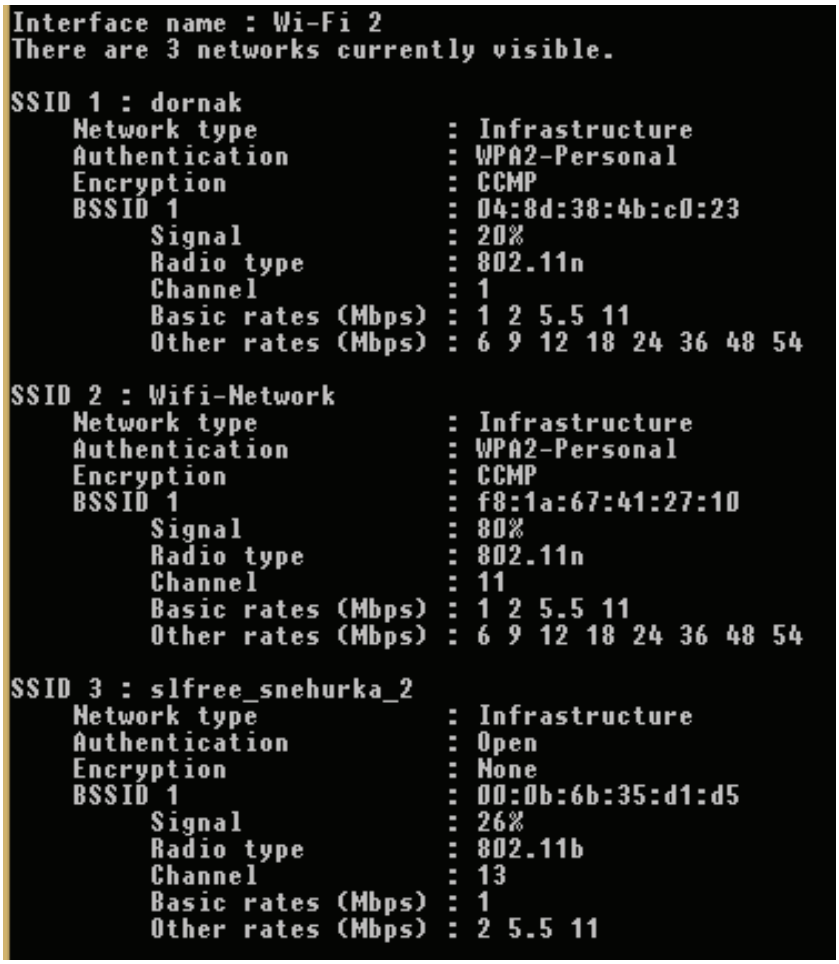
Network shell (**netsh**) je nástroj příkazového řádku, který umožňuje nastavit a zobrazit stav různých síťových komunikacích bežící na zařízeních.

Příkazy **netsh** pro bezdrátové lokální sítě (WLAN) slouží ke konfiguraci nastavení bezdrátové sítě 802.11 připojení a zabezpečení pro počítače se systémem Windows. Balíček příkazů netsh obsahuje také možnost sledování a analýzy bezdrátové sítě.

Následující příkaz zobrazí dostupné wifi sítě a jejich nastavení např. typ sítě, úroveň signálu, kanály atd. (viz. obr. 3.25).

```
netsh wlan show network mode=bssid
```

Výpis 5: Ukázka použití příkazu netsh



Obrázek 3.25: Network shell - Ukázka výstupu po provedení netsh příkazu

3.2.2 InSSIDer v2.1 [24]

inSSIDer v. 2.1 je open-source program, který skenuje sítě v dosahu počítače Wi-Fi anténou, sílu signálu v průběhu času a určuje jejich bezpečnostní nastavení (včetně toho, zda jsou nebo nejsou chráněné heslem).

Obrázek 3.26: InSSIDer v2.1

3.2.2.1 Funkce programu Program InSSIDER nabízí několik informací o přístupových bodech v okolí (viz. obr. 3.27):

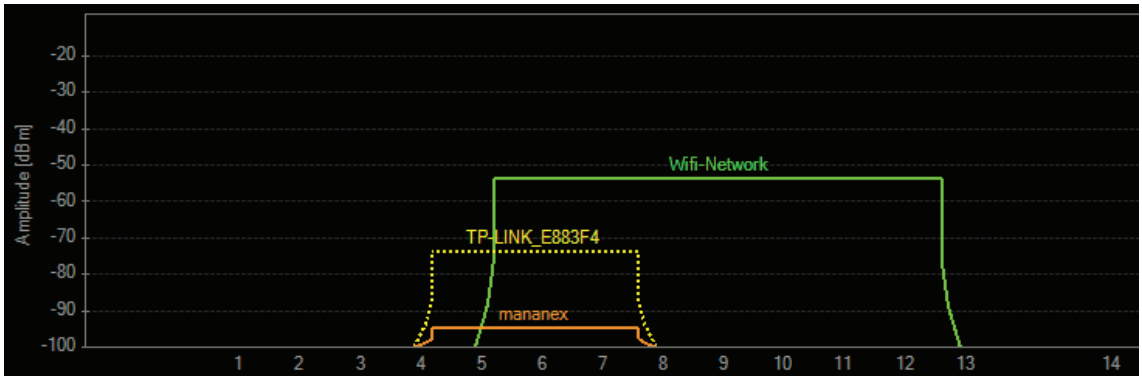
- **SSID** - název sítě
- **Channel** - kanál, na kterém síť pracuje
- **RSSI** - úroveň signálu
- **Security** - použité zabezpečení sítě
- **MAC Address** - MAC adresa přístupového bodu
- **Max Rate** - maximální výkon AP
- **Vendor** - výrobce zařízení
- **Network Type** - typ sítě

Nástroj dále umožňuje zobrazovat jednotlivé grafy, které zobrazují sílu přijímaného signálu v čase (viz. obr. 3.28) a nebo zobrazují bezdrátové sítě s použitými kanály (viz. obr. 4.4).

SSID	Channel	RSSI	Security	MAC Address	Max Rate	Vendor	Network Type
Wifi-Network	**11 + 7**	**-54**	**WPA2-Personal**	**F8:1A:67:41:27:10**	**150**		**Infrastructure**
slfree_snehurka_2	13	-95	Open	00:0B:6B:35:D1:D5	11	Wistron Neweb C...	Infrastructure
TP-LINK_E883F4	6	-90	Open	00:21:27:E8:83:F4	54	TP-LINK Technol...	Infrastructure
mananex	6 + 2	-95	WPA2-Personal	14:D6:4D:7D:0D:36	150	D-Link International	Infrastructure

Obrázek 3.27: InSSIDer - Přehled dostupných bezdrátových sítí

Obrázek 3.28: InSSIDer - Úroveň přijímaných signálů



Obrázek 3.29: InSSIDer - Bezdrátové sítě s použitými kanály

4 Monitoring a analýza bezdrátových síti

Obecně se dá říci o analýze bezdrátových sítí, že se zaobírá monitoringem a následným vyhodnocování provozu těchto sítí. Touto metodou lze odhalit problémy nebo bezpečnostní rizika sítí.

Samotná analýza probíhá pomocí „sofwarových"nástrojů. Tyto nástroje zachycují pakety procházející sítí. Hlavní funkce těchto programů je analýza zachycených paketů (dat) a to jak z hlediska druhu přenášených dat nebo komunikačních protokolů. A následovné použití různých filtrů.

Sledování sítě lze provádět v dlouhých nebo v krátkých intervalech. V případě krátkých intervalů uživatel (správce sítě) analyzuje aktuální získané data například:

- vytížení sítě,
- velikost přenášených dat,
- aktuálně zachycené pakety.

Často se zaměřuje sledování na konkrétní problém. Z hlediska dlouhodobé analýzy správce sítě získává výsledky sledování sítě za několik desítek dnů. Tyto informace můžou vypovídat například:

- o výpadcích sítě,
- o neoprávněných přístupů do sítě,
- o chybách nastavení.

Údaje z paketových „snifferů"můžou být zobrazeny do grafů, které pak můžou odhalit konkrétní problém v síti.

Nejdříve před samostatným monitoringem a analýzy provozu bezdrátové sítě je třeba uvést bezdrátovou kartu do správného režimu. Síťovou kartu je nutno přepnout do monitorovacího režimu (monitor mode). Toto řešení umožní pasivně sledovat chod bezdrátové sítě bez nutnosti připojení se na konkrétní síť. Karta zachycuje veškerý provoz na síti díky ní můžeme provést analýzu.

Následující příkazy uvedou bezdrátovou kartu do monitorovací režimu a nastaví kanál sítě.

```
iwconfig  wlan0 mode monitor
iwconfig  wlan0 channel 5
 ifconfig  wlan0 up
```

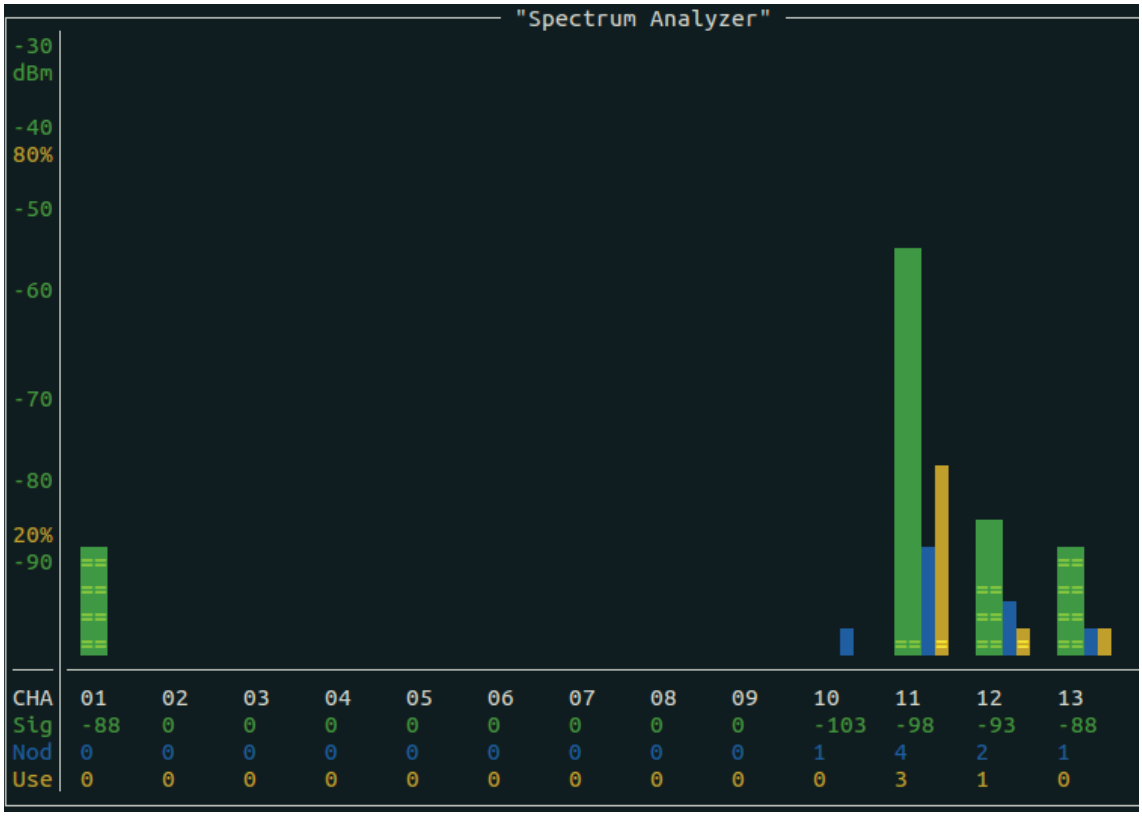
Výpis 6: Ukázka nastavení bezdrátové karty

4.1 Sledování a analýza bezdrátového provozu [25]

Nástroje, které jsou v této práci uvedeny, nabízejí různé možnosti nějakého sledování a analýzy sítě. Některé nástroje jsou téměř totožné (např. Kismet a horst) a nebo se navzájem doplňují. Obecně lze říci, že při kombinaci více programů lze lépe provést analýzu.

Při testování byla síť používaná klienty, kteří používali síť běžným způsobem.

Jedna z možností sledování a pak provedení následné analýzy je sledování vytížení sítě. Toto demonstruje následující obrázek. Na obrázku lze vidět několik kanálů. V tomto případě se sledoval kanál 11, na kterém pracovala pouze jedna síť. Lze vidět aktuální vytíženost sítě, počet uzlů a nebo signál sítě. Na základě těchto údajů může správce odhalit neoprávněný provoz, problémy na sítí, což vede pak k lepšímu nastavení přístupového bodu.

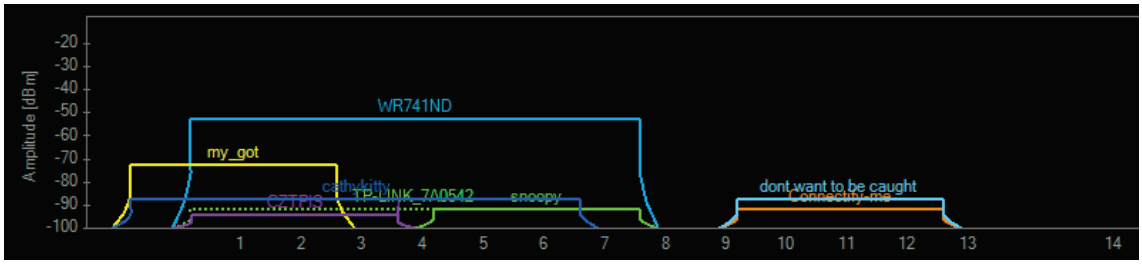


Obrázek 4.1: horst - Zobrazení kanálů a vytížení sítě

Tuto možnost sledování a analýzy sítě umožňuje většina popsaných nástrojů v této práci.

Bezdrátové sítě 802.11 pracují v pásmech 2,4 GHz a 5 GHz. Každé toto pásmo je rozděleno na několik kanálů, které jsou odděleny. U 2,4 GHz pásma je kanálů 14 a několik z nich se kryje. Problém nastává v tom okamžiku, kdy jednotlivé přístupové body pracují na stejné kanálu a pak může docházet k vzájemnému rušení. Tento problém lze snadno odhalit nejlépe pomocí programů InSSIDer (viz. kap. 3.2.2) a LinSSID (viz. kap. 3.1.7) s

využitím kanálového analyzátoru, který umožňuje graficky zobrazit kanály a vede pak k lepší optimalizaci bezdrátových sítí viz. následující obrázek.



Obrázek 4.2: InSSIDer - Zobrazení kanálů

Několik nástrojů popsaných v této práci umožňuje sledování a analýzu protokolů sítě. Obrázek 4.3 demonstruje samotný provoz a zobrazení paketů či protokolů. Můžeme zde vidět například:

- detekování nové sítě (BEACON)
- informace o spojení (ACK, RTS, CTS)
- zachycení používání sítě uživatelem (UDP protokol, QDATA)

```
CH-Sig-RT-SOURCE            (BSSID)             TYPE    INFO
32 -00   1 f8:1a:67:41:27:10 (f8:1a:67:41:27:10) QDATA   ENCRYPTED
31 -98   2 00:00:00:00:00:00 (00:00:00:00:00:00) UNKNOW
32 -00   1 f8:1a:67:41:27:10 (f8:1a:67:41:27:10) QDATA   ENCRYPTED
31 -98   2 00:00:00:00:00:00 (00:00:00:00:00:00) ACK     f8:1a:67:41:27:10
32 -00   1 f8:1a:67:41:27:10 (f8:1a:67:41:27:10) QDATA   ENCRYPTED
31 -98   2 00:00:00:00:00:00 (00:00:00:00:00:00) ACK     f8:1a:67:41:27:10
31 -98   2 f8:2f:a8:ff:64:55 (00:00:00:00:00:00) RTS     f8:1a:67:41:27:10
31 -98   2 00:00:00:00:00:00 (00:00:00:00:00:00) CTS     f8:2f:a8:ff:64:55
32 -00   1 f8:2f:a8:ff:64:55 (f8:1a:67:41:27:10) QDATA   ENCRYPTED
31 -98   2 00:00:00:00:00:00 (00:00:00:00:00:00) UNKNOW
31 -93   2 f8:1a:67:41:27:10 (f8:1a:67:41:27:10) BEACON  'Wifi-Network' 44322b68180
31 -93   2 f8:1a:67:41:27:10 (f8:1a:67:41:27:10) BEACON  'Wifi-Network' 44322b81180
31 -88   2 00:0b:6b:35:d1:d5 (00:0b:6b:35:d1:d5) UDP     92.223.1.121 -> 10.143.69.149
31 -88   2 00:00:00:00:00:00 (00:00:00:00:00:00) ACK     00:02:72:68:2f:dc
31 -88   2 00:0b:6b:35:d1:d5 (00:0b:6b:35:d1:d5) BEACON  'slfree_snehurka_2' 28c6b4e3181
```

Obrázek 4.3: horst - Zobrazení zachycení provozu

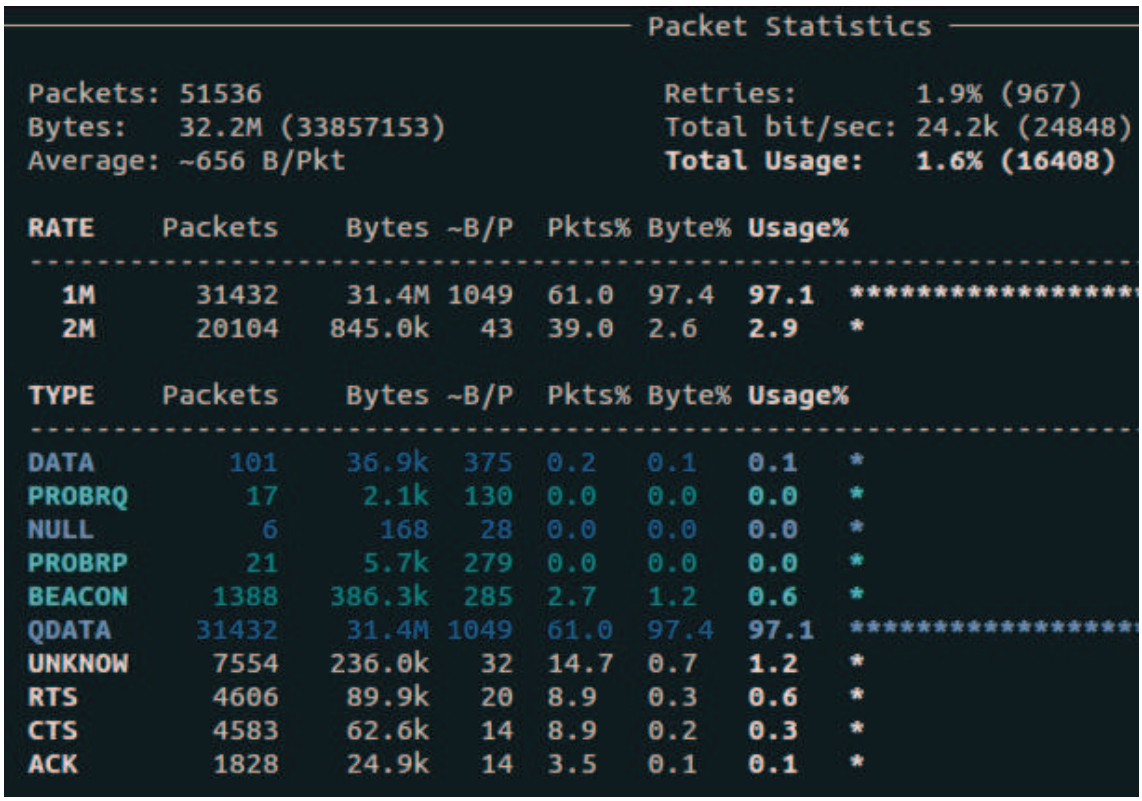
Tuto možnost nejlépe vystihují nástroje Kismet, horst a nebo Wireshark. Nejlepší protokolovou analýzu nabízí program Wireshark, který je dosud nejpoužívanější nástroj pro tyto účely.

Pro paketovou analýzu lze využít možnost zobrazení celkové paketové statistiky. Tohle je vidět v níže uvedeném obrázku, kde je použit pro demonstraci nástroj horst. V této statistice lze najít například:

- celkový počet zachycených paketů,

- průměrnou velikost paketů,
- počet opakovacích paketů,
- celkové využití,
- různé druhy protokolů se statistikami např. procentuální využití v síti,

a spoustu dalších informací z kterých lze provést analýzu.



Obrázek 4.4: horst - Paketové statistiky

Tyto informace mají velké využití při dlouhodobém sledovaní. Z těchto informací se provede analýza, které můžou odhalit problémy a pro lepší přehlednost je možnost zobrazit údaje do grafů.

Z hlediska sledování základní parametrů sítě lze zmíněnými nástroji získat informace o bezdrátové síti například SSID, MAC adresu, signál, kanál, frekvence, přenosovou rychlost, typ sítě a nebo o počtu klientech připojených na danou síť atd..

Programy jako Kismet, horst a zejména Wireshark nabízejí několik funkcí k provedení analýzy bezdrátového provozu, včetně použití filtrů, detailního rozboru protokolů a samotné dešifrování provozu sítí.

Před samotnou analýzou je třeba získat zachycené pakety. Analýzu lze provést dvěma možnostmi:

- rovnou z aktuálních zachycených paketů (z živého rozhraní),
- nebo načíst pakety ze souboru (dlouhodobé zachytávání paketů) a provést analýzu.

V tomto případě byla zvolena možnost druhá. V dané oblasti s přístupovými body bylo spuštěno zachytávání dat a výsledný počet zachycených paketů byl cca 260 000. Z tohoto množství paketů byla následně provedena analýza bezdrátového provozu. Testovací topologií byla infrastrukturální síť.

4.1.1 Význam filtrů

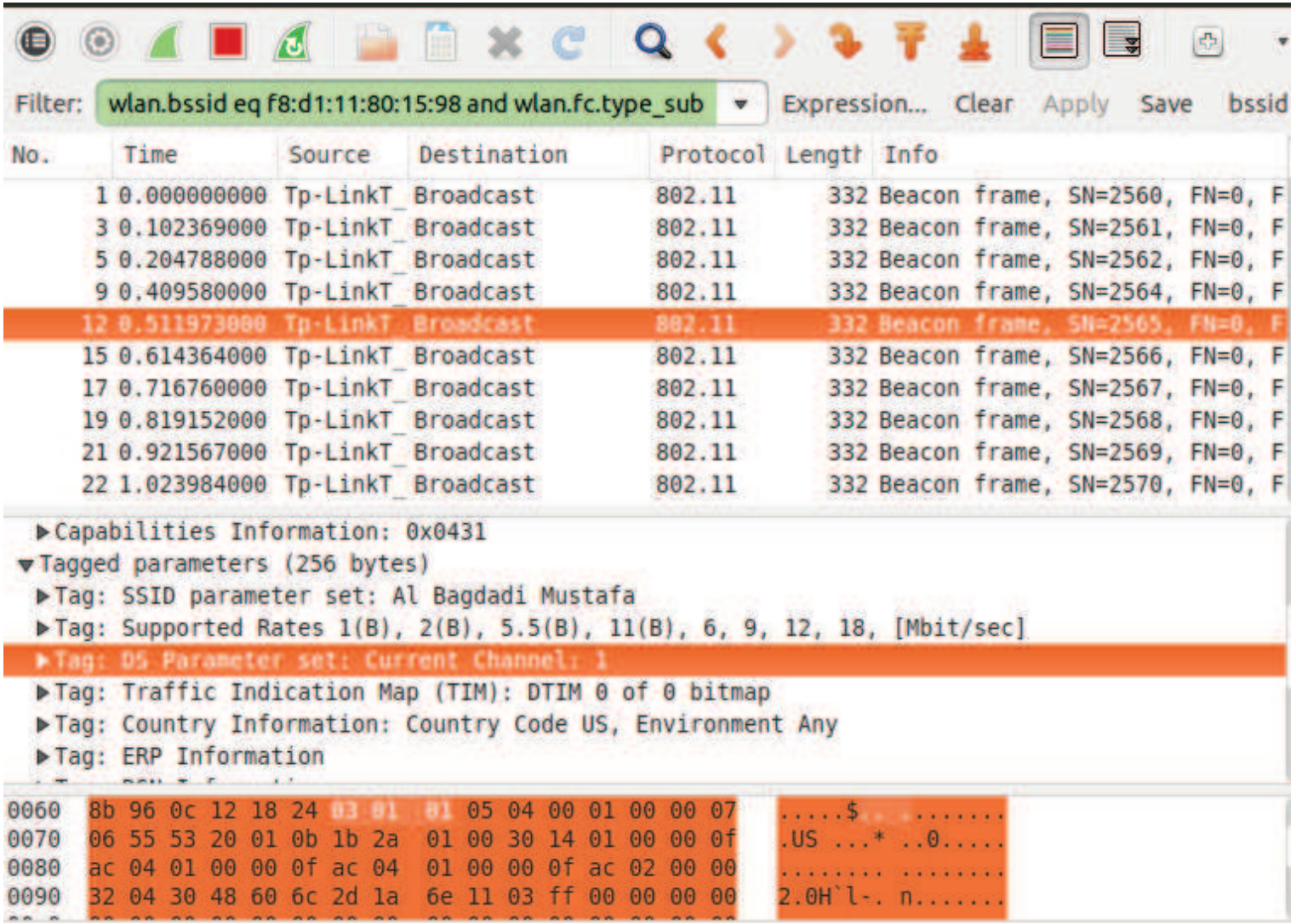
Při zachytávání provozu sítě dochází k získání velkému množství dat. Jelikož analýza je většinou zaměřena na konkrétní problém, tak lze využít těchto zobrazovacích filtrů. Díky filtrům můžeme snadno zobrazit užitečné data a zaměřit se na daný problém aniž bychom prohledávali veškerá zachycená data.

4.1.2 Zjištění kanálu přístupového bodu

Pomocí programů lze získat kanál vysílací stanice. V případě, že známe SSID stanice můžeme pomocí Wiresharku následujícím filtrem zjistit kanál stanice:

```
wlan.bssid eq f8:d1:11:80:15:98 and wlan.fc.type_subtype eq 8
```

Na řádku se nám zobrazí informace o zdrojové, cílové adrese a SSID sítě. Při kliknutí na **IEEE 802.11 Wireless LAN Management Frame - Tagged Parameters - Tag: DS Parameter Set** můžeme zjistit obsah této části, která nám zobrazí číslo kanálů přístupového bodu (viz obrázek 4.5).

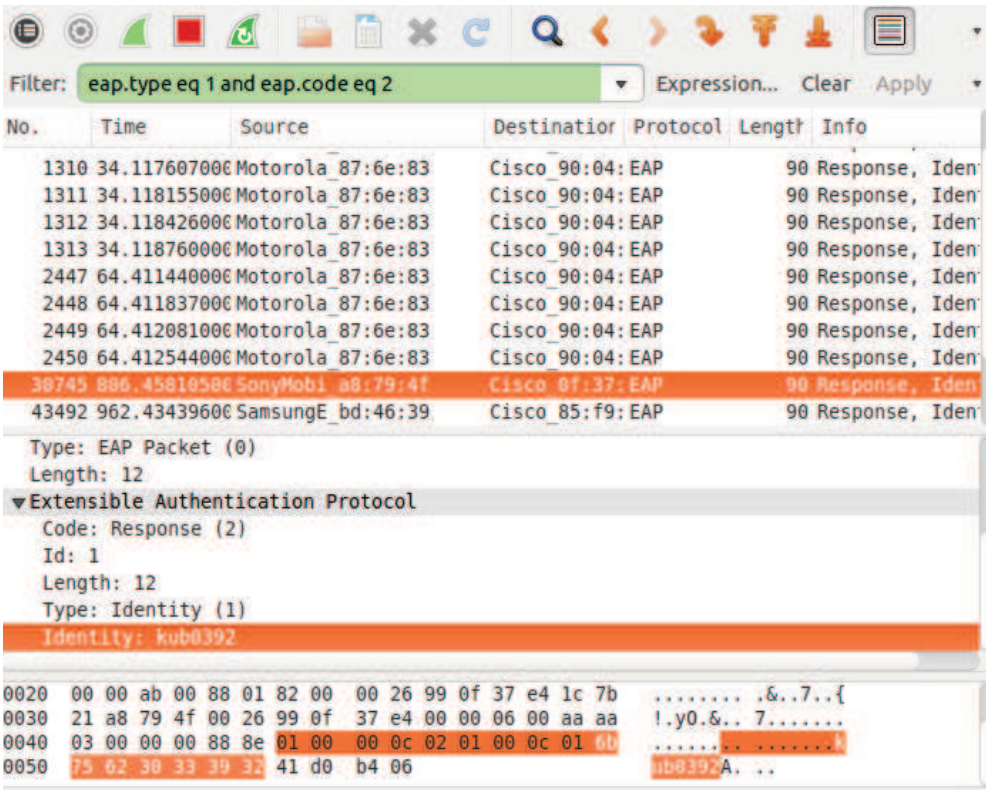


Obrázek 4.5: Wireshark - zjištění kanálu

4.1.3 Identifikace protokolu EAP

Protokol Extensible Authentication Protocol (EAP) používá ověřovací mechanismy se spojení s IEEE 802.1x pro ověření uživatelů pomocí metod EAP. Pomocí např. Wiresharku můžeme toto ověřování zachytit včetně identity, výměny dat nebo informace o úspěchu či neúspěchu ověření.

Následující obrázek 4.6 zobrazuje odpověď na *EAP Request* a zároveň odhaluje identitu formou uživatelského jména *kub0392*.



Obrázek 4.6: Wireshark - Odhalení identity EAP

Získání identity uživatele může být základ pro útok na bezdrátovou síť.

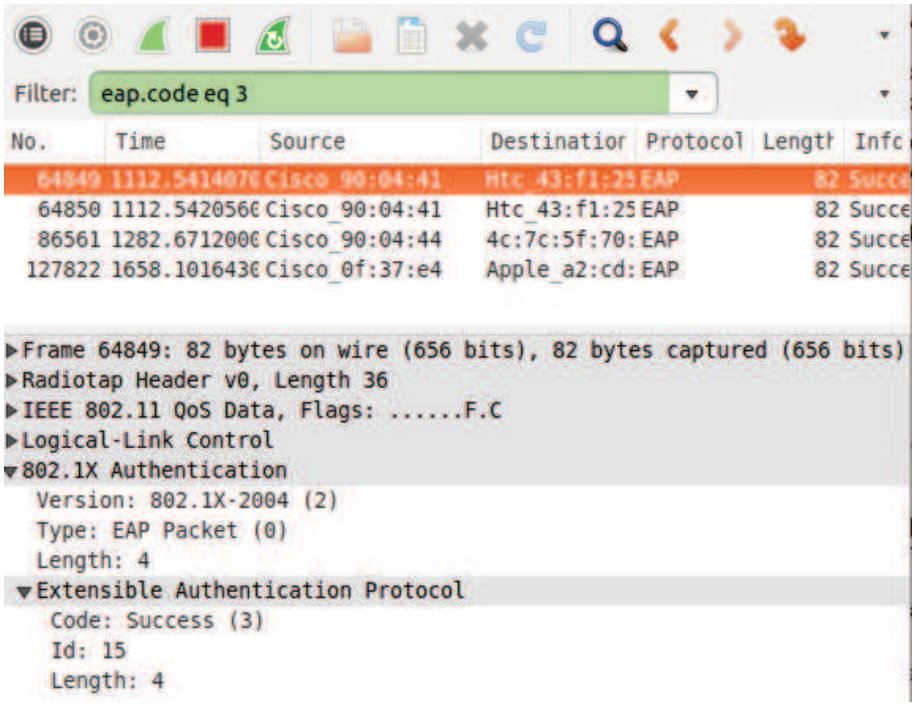
S ověřováním na bezdrátových sítí se často zjišťuje zda nedochází k selhání na straně nebo klienta. Pomocí filtru:

```
eap.code eq 3
```

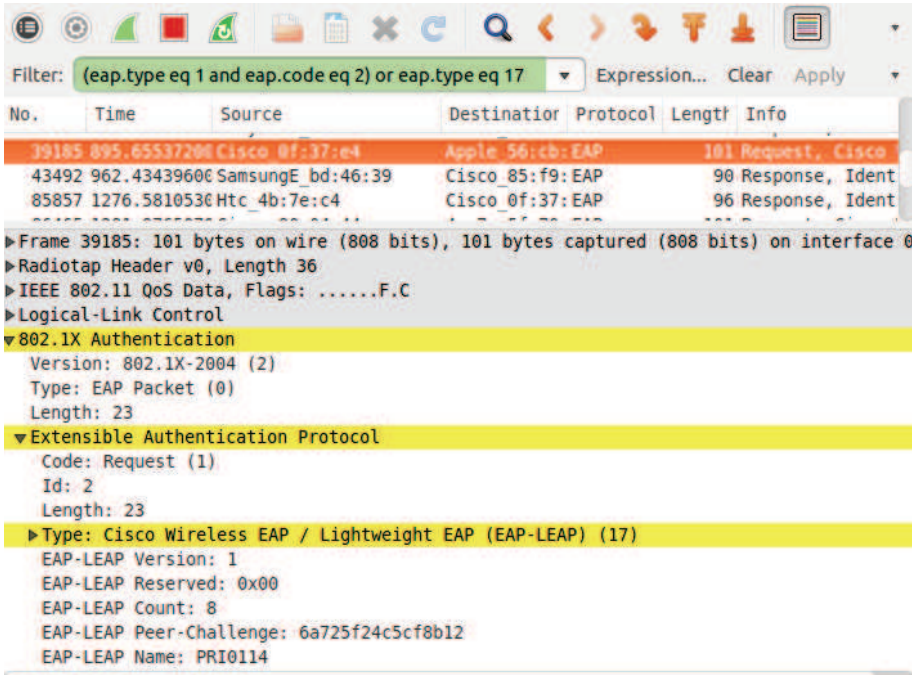
lze zjistit zda ověření bylo úspěšné. Ukázka tohoto filtru na zachycených paketech je zobrazen na obrázku 4.7.

Pokud bychom chtěli zjistit selhání ověřování lze použít filtr:

```
eap.code eq 4
```



Obrázek 4.7: Wireshark - Oznámení o úspěchu EAP



Obrázek 4.8: Wireshark - Odhalení identity Cisco LEAP

4.1.4 Identifikace protokolů TKIP a CCMP

Hlavička šifrovacích protokolů se nachází za IEEE 802.11 hlavičkou. Z této hlavičky lze získat informace zda je použit TKIP nebo CCMP. Pro zjištění protokolů TKIP nebo CCMP můžeme použít např. u Wiresharku následující filtry:

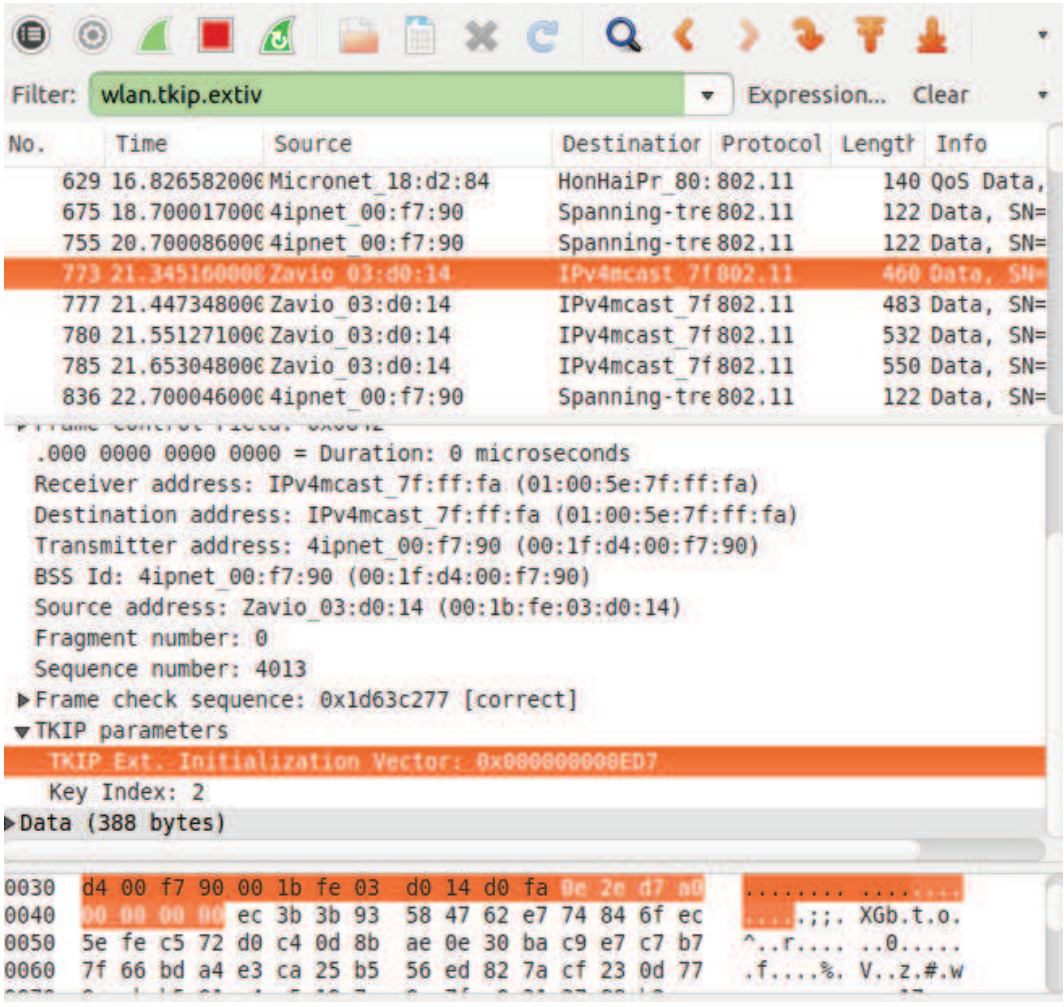
Pro TKIP:

```
wlan.tkip.extiv
```

Pro CCMP:

```
wlan.ccmp.extiv
```

Po následném prozkoumání hlavičky lze zjistit přítomnost TKIP nebo CCMP viz. obrázek 4.9, kde je zobrazen protokol TKIP s jeho parametry.

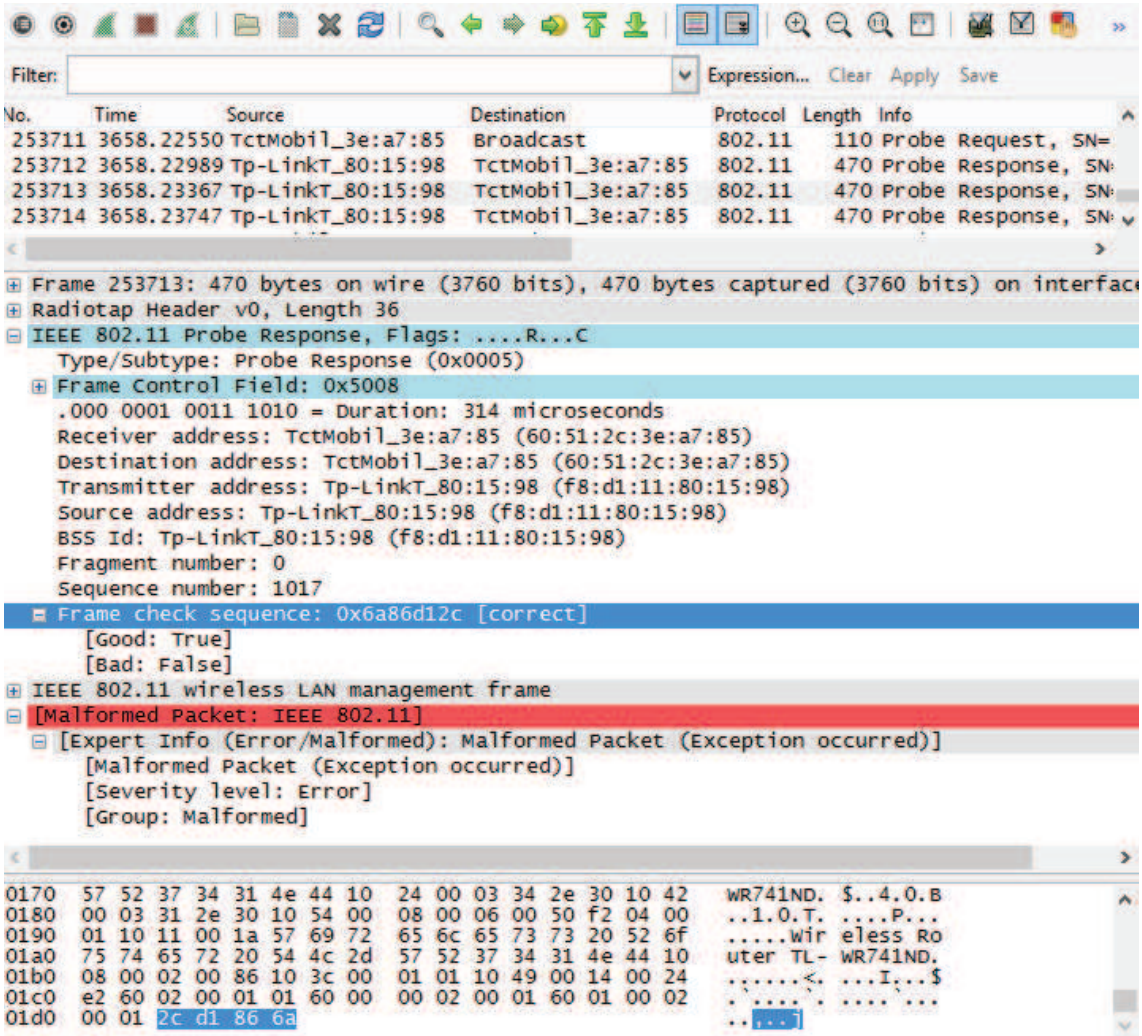


Obrázek 4.9: Wireshark - Identifikace provozu TKIP

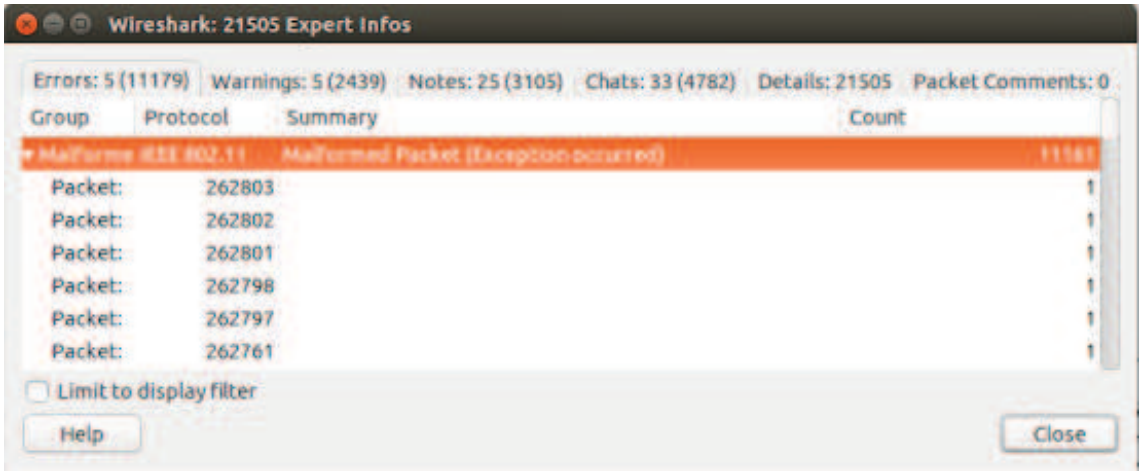
4.1.5 Analýza poškozeného datového provozu

V průběhu zachytávání dat se v obsahu objeví podezřelé chování. Toto lze pomocí Wiresharku odhalit pomocí expertní analýzy, která zobrazí deformované data. Následující obrázek 4.11 zobrazuje 11161 poškozených paketů.

Pokud se někde objeví hláška „Malformed paket", tak daný zachycený paket není v souladu s pravidly IEEE 802.11 a veškeré další zpracování obsahu paketu je zastaveno. Takto označené pakety mohou označovat neoprávněnou aktivitu uživatele (útočníka), fuzz testování a nebo mohlo dojít k poškození během přenosu rámce. Chyba může být taky na straně vysílající stanice, která posílá již deformované rámce. V takovém případě zkontrolujeme **Frame Check Sequence** (FCS), kde snadno zjistíme co deformaci způsobilo.



Obrázek 4.10: Wireshark - Zobrazení neplatného rámce



Obrázek 4.11: Wireshark - Expertní analýza

4.1.6 Analýza bezdrátového provozu stanic

V dnešní době existuje řada útoků na bezdrátové sítě. Jedním z nich může být útok typu „spoofing", kdy útočník začne vysílat data do sítě pod existujícím „jménem"stanice, která v síti pracuje.

Proto je třeba zjistit cestu rámce v bezdrátové síti. Pomocí Wiresharku můžeme prozkoumat stav distribučního systému v **IEEE 802.1 1 - Frame Control - Flags**. Pomocí následujícího filtru lze se zaměřit na tento problém:

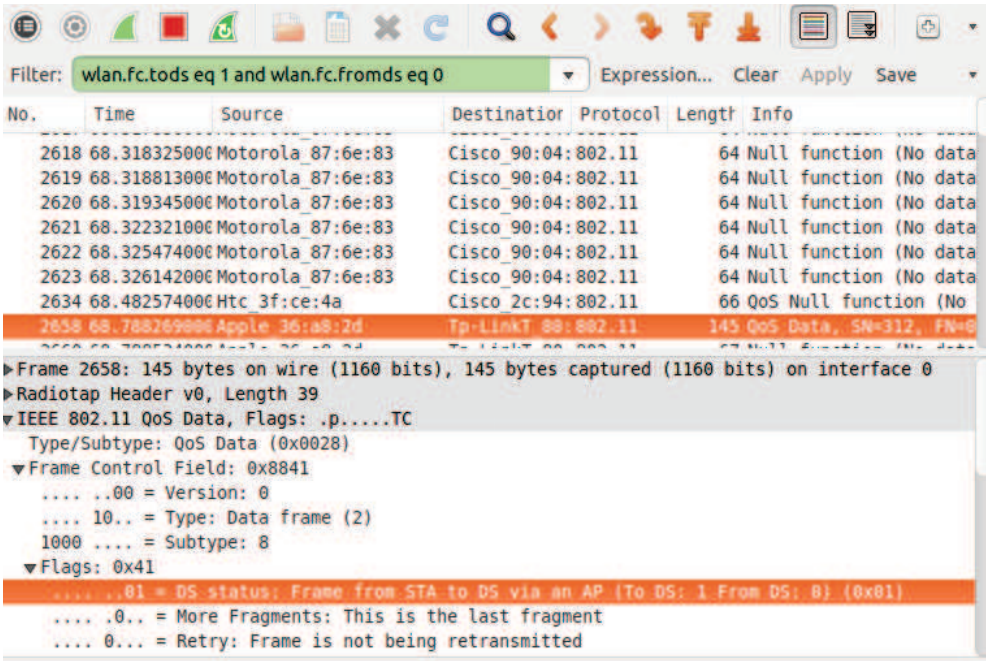
```
wlan.fc.tods eq 1 and wlan.fc.fromds eq 0
```

Pokud se podíváme na pole *DS status*, lze zjistit cestu rámce. Na obrázku 4.13 vidíme, že rámec je vysílán přímo distribučnímu systému tzn. rámec je přenesen bezdrátovou stanicí „APčku". Toto však nemusí znamenat případný útok, a proto je třeba zvýšit pozornost pořadovým číslům rámců.

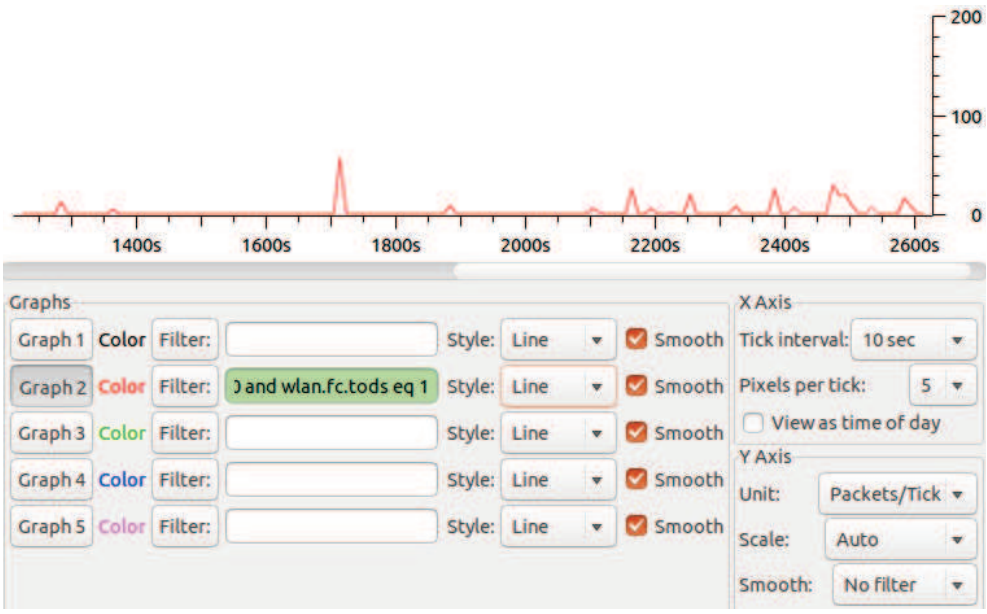
Pro lepší přehlednost lze zobrazit data do grafů. Obsah dat se dá opět vyfiltrovat a zobrazit do grafů. Příkladem je následující filtr, který informuje o datovém provozu ze stanic k přístupovému bodu:

```
wlan.fc.fromds eq 0 and wlan.fc.tods eq 1
```

Výsledek použití filtru u grafů je znázorněn na obrázku 4.13. Kde je vidět počet paketů vysílaných ze stanice „APčku".



Obrázek 4.12: Wireshark - Provoz bezdrátových stanic



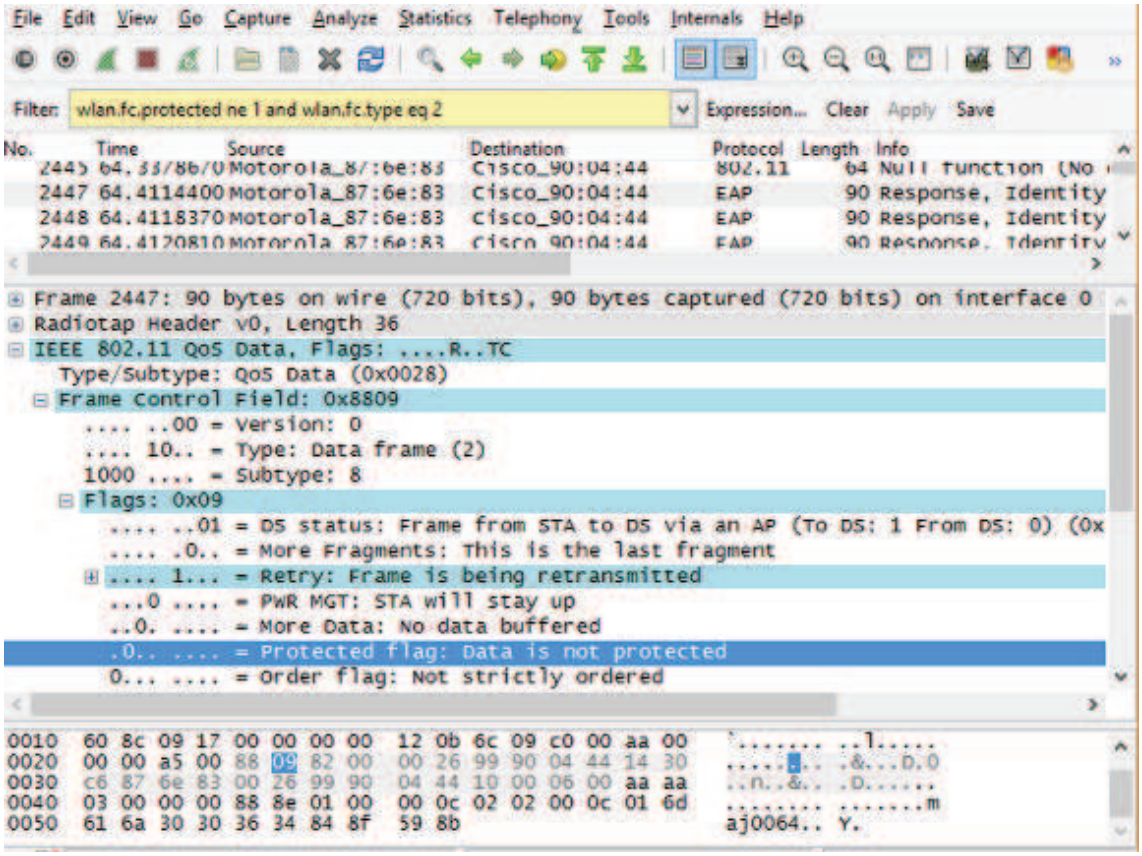
Obrázek 4.13: Wireshark - Analýza provozu

4.1.7 Nešifrovaný provoz

Často se v bezdrátových sítích objevuje nešifrovaný provoz. Nešifrovaný provoz může znamenat špatnou konfiguraci sítě a pak může docházet k odposlechům a získání citlivých informací. Pomocí následujícího filtru, lze zobrazit nešifrovaný provoz:

```
wlan.fc.protected ne 1 and wlan.fc.type eq 2
```

Tento filtr identifikuje nešifrované datové rámce, které jsou pro analýzu tohoto problémů důležité. Výsledek zmíněného filtru může vidět na obrázku 4.14. Můžeme vidět, v kontrolním rámci je *protected bit* nastaven na *0*, což znamená nešifrovaný provoz rámce. V opačném případě je bit nastaven *1*.



Obrázek 4.14: Wireshark - Nešifrovaný provoz

Na obrázku si můžeme všimnout, že rámec byl znova přeposlán. To mohlo znamenat, že vznikl zdroj interference v bezdrátové síti, který braní ke správnému doručení předešlých rámců.

4.1.8 Dešifrování provozu

Veškerý zachycený provoz sítě je nějakým způsobem šifrován. Kvůli šifrování jsme částečně omezeni provádět analýzu paketů a odhalovat problémy sítě. Díky Wiresharku tak lze dešifrovat několik desítek protokolů, ale potřebujeme mít k dispozici správné klíče (WEP, WPA/WPA2). Pokud jsme administrátorem sítě, tak lze tyto klíče snadno zjistit. Avšak existuje možnost prolamování těchto klíčů např. pomocí nástroje Aircrack-ng. Prolamování klíčů není legální činnost a pachatel může být stíhán.

Pro testování byla zvolena vlastní síť a klíče byly zjištěny v nastavení přístupového bodu.

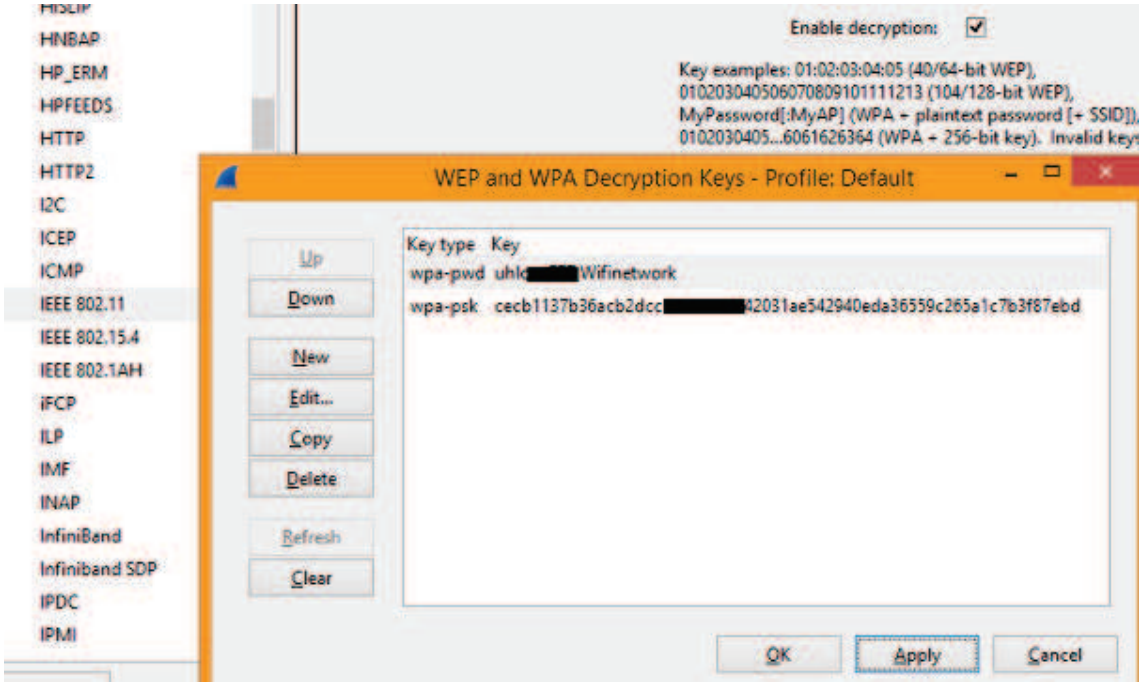
Nastavení klíčů ve Wiresharku pro dešifrování provozu klikneme na **Edit - Preferences - IEEE 802.11**. V okně zaklikneme **Enable Decryption** a pak vložíme klíče v různých formátech například:

Pro WPA:

```
wpa-pwd:HESLO:MojeSSID
```

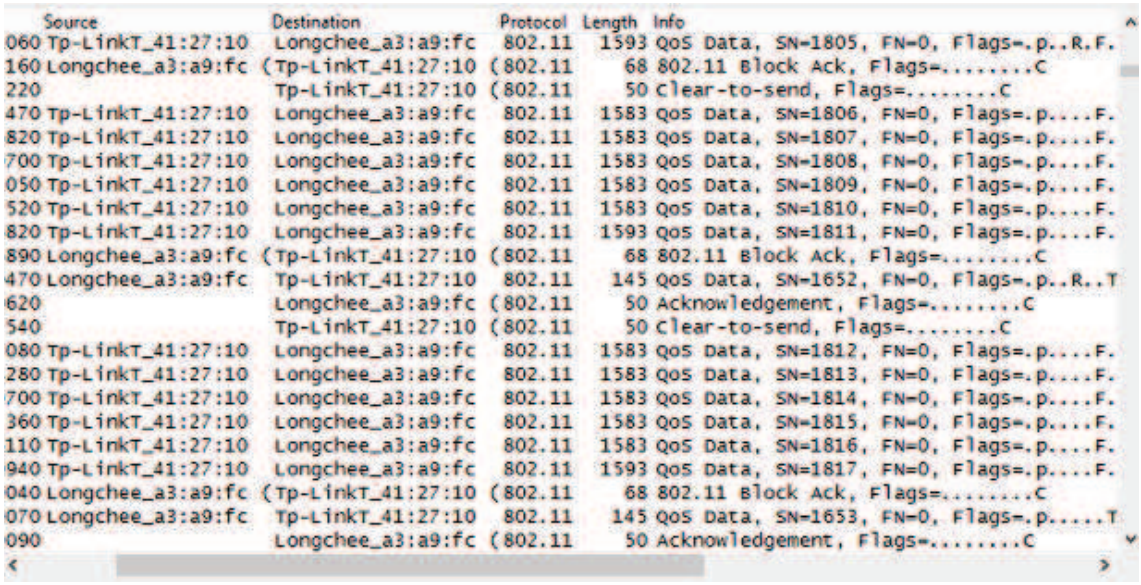
```
wpa-psk:123456789acdef...6569686
```

Následující obrázek 4.15 demonstruje nastavení klíčů, které bylo při dešifrování použito.

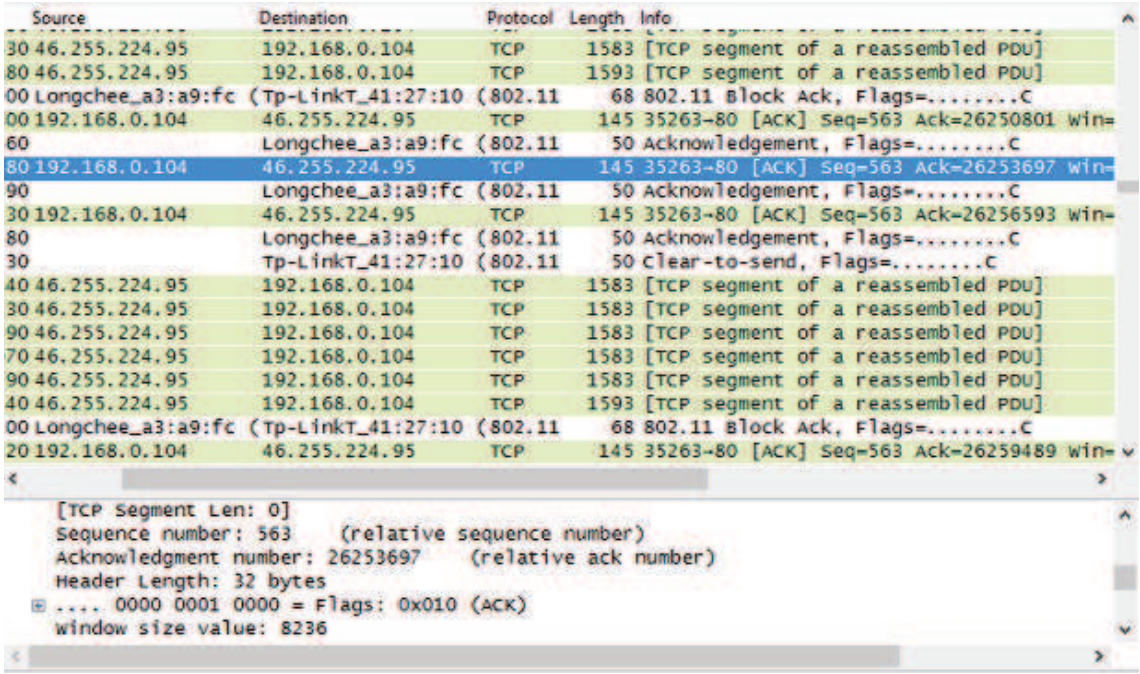


Obrázek 4.15: Wireshark - Zadávání klíčů

Po potvrzení klíčů Wireshark dešifruje provoz. Po dešifrování můžeme provést rozbor jednotlivých rámců a získat potřebné informace (zdrojové a cílové adresy IP adresy, handshake, potvrzení přijmu ACK apod.) Ukázka šifrovaného a následně dešifrovaného provozu lze vidět na obrázcích 4.16 a 4.17.



Obrázek 4.16: Wireshark - Zašifrovaný provoz sítě



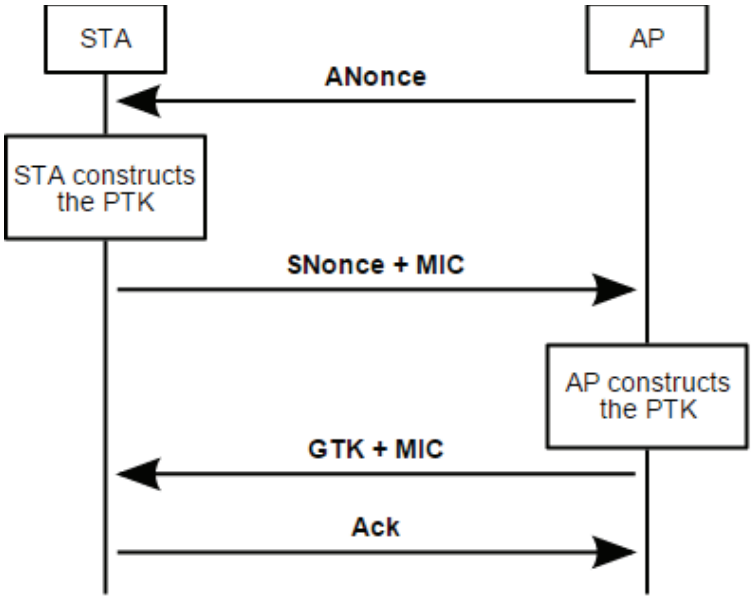
Obrázek 4.17: Wireshark - Rozšifrovaný provoz sítě

4.1.9 Zachycení handshake [27]

Čtyřcestný handshake je typ síťového ověřování sítě stanoveným IEEE 802.11i. Poskytuje bezpečnou strategii ověřování pro data přenášené přes síťovou architekturu.

Princip čtyřcestného handshake:

- AP pošle hodnotu pro klienta (ANonce). Klient získal všechny atributy k vytvoření PTK (Pairwise Transient Key)
- Klient posílá hodnotu (SNonce) přístupovému bodu spolu s MIC (Message authentication code), včetně ověření.
- Přístupový bod vysílá GTK (Group Temporal Key) a pořadové číslo spolu s jiným MIC. Tato číselná řada se použije v následujícím vysílání rámce (Multicast nebo Broadcast), takže přijímající stanice může provádět základní detekce opakování.
- Klient pošle potvrzení potvrzení přístupovému bodu, že je vše v pořádku.

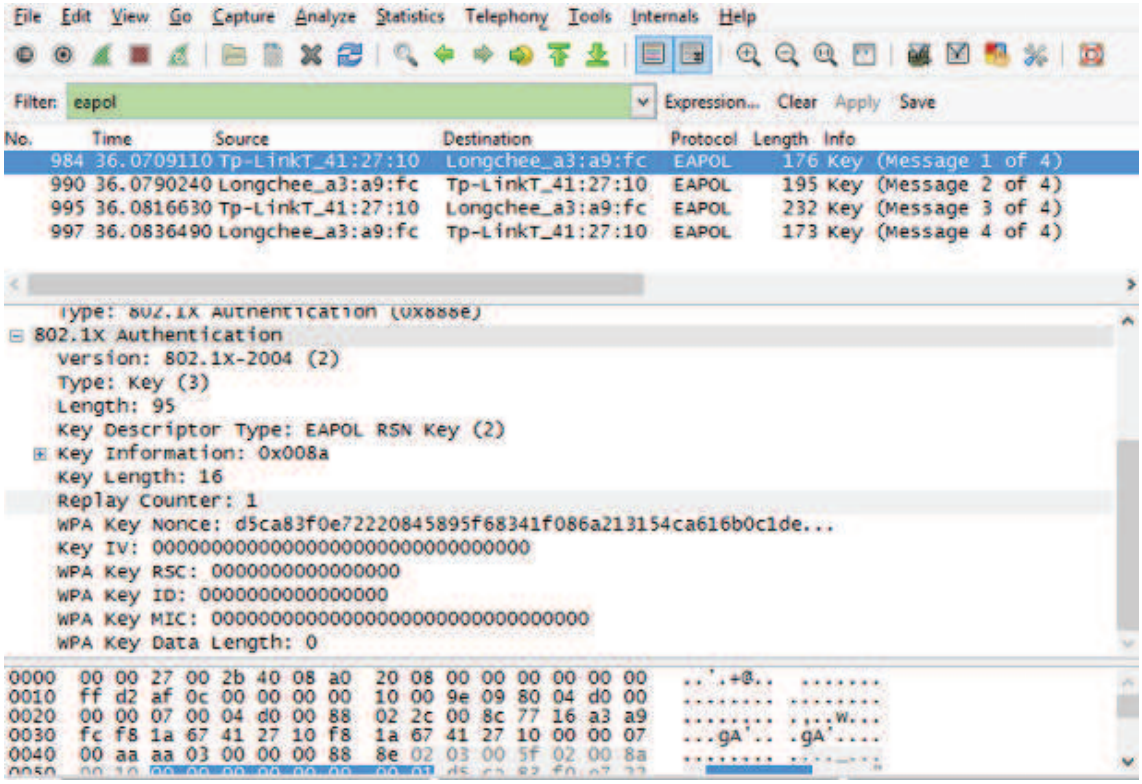


Obrázek 4.18: Princip čtyrcestného handshake [27]

Pomocí následujícího filtru lze ve Wiresharku zachytit handshake:

```
eapol
```

Výsledek filtru můžeme vidět za obrázku 4.19, kde jsou zobrazeny čtyři handshake zprávy, včetně zachycení reálné autentizace mezi klientem a přístupovým bodem.



Obrázek 4.19: Wireshark - Zachycení čtyrcestného handshake

5 Porovnáni nástrojů pro monitoring a analýzu bezdrátových síti

Každý zvolený open-source nástroj určený pro monitoring a analýzu bezdrátové sítě je porovnán s nástrojem Kismet (viz. kap. 3.1.2) a zároveň je nástroj otestován pro zmíněné účely.

5.1 Porovnání iwlist a nm-tool s nástrojem KISMET

Obecně lze říct o iwlist a nm-tool, že jsou základními nástroji pro získaní informací o sítích. U těchto nástrojů lze použitím jednoduchých příkazů zjistit informace jako např.

- MAC adresa AP
- SSID
- Frekvence, na kterém AP pracuje
- Topologie sítě (např. AD-HOC)
- Zabezpečení sítě
- Bit rate

V porovnání s Kismetem tyto nástroje nabízejí „zlomek"možnosti jak zjistit nějaké informace o bezdrátových sítí. Avšak nalezené základní údaje o síti pro běžné uživatele jsou dostačující. Jelikož tyto zmíněné nástroje se ovládají pomocí příkazů, tak lze veškeré informace exportovat do souboru např. textový nebo logovací soubor.

5.2 Porovnání Network shell s nástrojem KISMET

Network shell nabízí stejné možnosti získávaní informací o sítích jako je u nástrojů iwlist a nm-tool (viz. kap. 3.1.1). Avšak s rozdílem, že Network shell pracuje na platformě Windows. Pomocí příkazu lze získat opět základní informace o bezdrátových sítí např. signál, SSID, typ sítě, šifrování, atd. (viz. obr. 3.25).

Veškeré zjištěné informace lze jednoduše pomocí příkazu exportovat do souboru a v porovnání s Kismetem nástroj nenabízí grafické zobrazovaní grafů a zobrazuje pouze základní informace o bezdrátových sítích.

5.3 Porovnání Aircrack-ng s nástrojem KISMET

Dalším rozsáhlejším způsobem sledování sítě je soubor nástrojů z balíčku Aircrack-ng (viz. kap. 3.1.3). Pro analýzu sítě lze z baličku použít výhradně dva nástroje **airmon-ng** a **airodump-ng**. Ostatní nástroje jsou používány zejména pro testování nebo prolamování hesel zabezpečených sítí WEP, WPA.

Aby byla možné monitorování sítě je třeba bezdrátovou kartu uvést do monitorovací režimu a k tomu slouží právě zmíněný airmon-ng. Pro samotné sledování sítě je určen nástroj airodump-ng.

Jelikož z balíčku Aircrack-ng se pro monitoring a analýzu využívá jen pár nástrojů, tak nemůže konkurovat programu Kismet. V porovnání s Kismetem nabízí omezené možnosti sledování sítě. Nástroji lze sledovat parametry sítí např. BSSID, ESSID, přenesená data, použitý kanál, šifrování, úroveň signálu. Nástroje umožňují taky sledovat připojené klienty na síti (AP) a zjistit jejich MAC adresu, signál nebo počet přijatých paketů.

Aircrack-ng je konzolová aplikace a tudíž neumožňuje grafické výstupy jako u Kismetu. Pro další analyzování lze výstupy exportovat do souboru.

5.4 Porovnání programů InSSIDer v2.1 a LinSSID s nástrojem KISMET

Volně dostupné nástroje InSSIDer (viz. kap. 3.2.2) a LinSSID (viz. kap. 3.1.7) jsou velmi podobné programy pro sledování sítě. Rozdíl mezi nimi je že každý pracuje na jiném operačním systému.

Oba tyto programy nabízí uživatelsky přívětivé rozhraní, které jsou snadno ovladatelné. V porovnání s nástrojem Kismet tyto programy nabízejí pouze základní informace o bezdrátových sítí (např. SSID, MAC adresu AP, zabezpečení a nebo kanály). Kismet nabízí podrobnější informace o sítích. Porovnávané programy jsou spíše informativní a nenabízejí možnost např. zjistit počet přijatých paketů, chybových paketů nebo rozšířené možnosti úprav konfiguračního souboru.

Výhody	**Nevýhody**
Grafické rozhraní	Základní informace o bezdrátových sítí
Grafické zobrazení jednotlivých pásem	Omezené možnosti práce s bezdrátovými sítěmi
Grafické zobrazení využití jednotlivých kanálů	Omezené možnosti exportu informací do souboru
Vhodné běžného uživatele	Omezené možnosti jakékoliv zjištění podrobnějších informací o sítí

Tabulka 5.1: Výhody a nevýhody InSSIDer a LinSSID

5.5 Porovnání Wavemon s nástrojem KISMET

Další programem je Wavemon. Tento nástroj už má o něco blíže ke Kismetu. Skládá se z grafického rozhraní, umožňuje nastavení celého programu např. měřítka výstupních grafů (viz. obr. 3.18). Program obsahuje také konfigurační soubory s možností úpravy nastavení Wavemonu.

Zobrazuje rozsáhlejší informace o dostupné síti např. síla signálu, kvalita linky, použití standardu, ip nebo MAC adresa (viz.obr. 3.15). Stejně jako Kismetu, Wavemon nabízí možnosti zobrazení dostupných sítí se základními údaji (ESSID, SSID, kanál, frekvence) a možnosti zobrazení grafů.

V programu Wavemon nelze zobrazit informace o klientech, kteří jsou připojeni na danou sít. U grafů nelze zobrazit spektrum, které umožňuje Kismet zobrazit. Dále neumožňuje zobrazit detailní informace o paketech.

5.6 Porovnání Wireshark s nástrojem KISMET

Wireshark je velmi rozsáhlý paketový sniffer. Má velké využití nejen bezdrátové síťové komunikaci na rozdíl od Kismetu, který je výhradně určený pro zachytávání provozu sítí. Podporuje stovky protokolů a taky dešifrovat šifrovaná data. V porovnání s Kismetem, Wireshark nabízí detailnější informace např. o paketech, rámcích. Tyto nástroje podporují grafické výstupy, které se dají rozšířit různými pluginy např. zobrazení dostupnosti určitého protokolu v čase.

Velkou výhodou Wiresharku je rozsáhlá analýza rámců. Tuto možnost tento nástroj ze všech testovaných programů zvládá nejlépe. Nevýhodou Wiresharku může být větší velikost zabíraného místa na disku.

Ve výsledku jsou tyto nástroje velmi vhodné pro analyzování bezdrátových síti.

5.7 Porovnání horst s nástrojem KISMET

Další vhodný open-source nástroj pro monitoring a analýzu je Highly Optimized Radio Scanning Tool (horst). Tento program nabízí rozsáhlé možnosti zisku informací o sítích a je srovnatelný s nástrojem Kismet.

Porovnání nástroje s Kismetem:

- Programy lze ovládat pomocí příkazu a nebo pomocí grafického rozhraní. Kismet z tohoto pohledu je uživatelsky přívětivější.
- Programy nabízejí možnosti zobrazit detailnější informace o sítích než to bylo u již zmíněných nástrojů. U horst nelze zobrazit informace o připojených klientech (u Kismetu lze).
- Nástroji lze získat detailní statistiky o paketech (paket rate, počet přenesených paketů za sekundu).
- Nástroje dále umožňují filtraci paketů.
- Nástroje mají velké možnosti zobrazení grafů např. zobrazení spektra, signál, paket rate, šum.
- Podporují client/server monitorování.

Ve srovnání s ostatními programy jsou nástroje **Wireshark**, **horst** a **Kismetem** nejvhodnější programy pro monitoring a analýzu z volně dostupných programů, které byly otestovány.

Závěr

S rostoucím počtem zařízení v bezdrátových sítí roste i potřeba tyto sítě sledovat a následnou analýzou odhalit bezpečnostní rizika.

Cílem práce bylo popsat bezdrátové sítě a možnosti sledování a analýzy provozu v těchto sítích. Pro monitoring a analýzu bylo vybráno několik open-source nástrojů:

- Kismet
- Wireshark
- Highly Optimized Radio Scanning Tool
- Wavemon
- Aircrack-ng
- InSSIDer a LinSSID
- iwlist, nm-tool a netsh

Tyto zmíněné nástroje byly otestovány z hlediska sledování a analýzy bezdrátových. Z výsledků testování dopadly nejlépe nástroje **Wireshark**, **Kismet** a **horst**. Těmito nástroji lze provést monitoring a důkladnou analýzu bezdrátových síti a tedy odhalit bezpečnostní rizika. Tyto nástroje je vhodné taky kombinovat např. Wireshark a Kismet (Kismetem zachytávat provoz sítě a pak následně zobrazit veškerá data ve Wiresharku a provést analýzu).

Ostatní zbylé programy jsou spíše zaměřeny na monitoring bezdrátových sítí. Lze nimi získat základní informace o sítích (SSID, kanál, typ sítě atd.) a nebo zobrazit např. úrovně signálu sítě v grafu. Programy jako LinSSID a InSSIDer dokáží zobrazit obsazenost kanálů frekvenčního pásma v dané oblasti.

Výše zmíněné open-source nástroje řeší dostatečně problém sledování a analýzy bezdrátových síti. Každý program je svým způsobem jiný a tudíž je vhodné je kombinovat k dosažení lepších výsledků.

Při vypracovaní byly získány rozsáhlé informace o fungování IEEE 802.11 bezdrátových sítí, které vedly autora práce k lepšímu pochopení problematiky.

Václav Durčík

Literatura

[1] HOLT, Alan a Chi-Yu HUANG, *802.11 wireless networks: security and analysis*, New York: Springer, c2010, xxi, 212 p. ISBN 1849962758

[2] GAST, Matthew, *802.11 wireless networks: the definitive guide*, 2nd ed. Sebastopol: O'Reilly, 2005, xxi, 630 s. ISBN 978-0-596-10052-0

[3] GAST, Matthew, *802.11n: a survival guide*, Sebastopol, CA: O'Reilly, c2012, 123 p. ISBN 1449312047

[4] GAST, Matthew, *802.11ac: a survival guide*, 1st ed. xvi, 133 pages. ISBN 978-1-449-34314-9

[5] CHANDRA, Praphul, *Wireless networking*, Boston: Elsevier/Newnes, c2008, xiii, 558 p. ISBN 07-506-8582-4

[6] LEMSTRA, W, Vic HAYES a John GROENEWEGEN, *The innovation journey of Wi-Fi: the road to global success*, New York: Cambridge University Press, 2011, xvi, 415 p. ISBN 05-211-9971-9

[7] ŠEBESTA, Roman a Marek DVORSKÝ, *Rádiové sítě I pro integrovanou výuku VUT a VŠB-TUO*, 1. vyd. Ostrava: Vysoká škola báňská - Technická univerzita Ostrava, 2014. ISBN 978-80-248-3612-6

[8] CSMA/CA. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2015-04-04]. Dostupné z: `http://cs.wikipedia.org/wiki/CSMA/CA`

[9] Aircrack-ng. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2015-04-04]. Dostupné z: `http://en.wikipedia.org/wiki/Aircrack-ng`

[10] Horst - lightweight wireless lan scanner and analyzer. [online]. [cit. 2015-04-04]. Dostupné z: `http://br1.einfach.org/tech/horst/`

[11] horst - Highly Optimized Radio Scanning Tool. [online]. [cit. 2015-04-04]. Dostupné z: `http://manpages.ubuntu.com/manpages/trusty/man8/horst.8.html`

[12] Scanning - How do I scan for Wireless Access Points? - Ask Ubuntu. [online]. [cit. 2015-04-04]. Dostupné z: `http://askubuntu.com/questions/75625/how-do-i-scan-for-wireless-access-points`

[13] Wavemon - a wireless network monitor application. [online]. [cit. 2015-04-04]. Dostupné z: `http://manpages.ubuntu.com/manpages/maverick/man1/wavemon.1.html#contenttoc3`

[14] Příkazy nástroje Netsh pro bezdrátovou místní síť (WLAN). [online]. [cit. 2015-04-04]. Dostupné z: `https://technet.microsoft.com/cs-cz/library/cc755301%28v=ws.10%29.aspx`

[15] Kismet. [online]. [cit. 2015-04-04]. Dostupné z: `https://www.kismetwireless.net/`

[16] Vysokovýkonný bezdrátový USB adaptér 150 Mbit/s TL-WN722N. [online]. [cit. 2015-04-04]. Dostupné z: http://cz.tp-link.com/products/details/?model=TL-WN722N#spec

[17] IEEE 802.11. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2015-04-04]. Dostupné z: http://cs.wikipedia.org/wiki/IEEE_802.11

[18] WPA and WPA2 (Wi-Fi security tutorial - part 2). [online]. [cit. 2015-04-04]. Dostupné z: http://www.maxi-pedia.com/wpa+wpa2+wifi+protected+access

[19] Symetrická šifra. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2015-04-04]. Dostupné z: http://cs.wikipedia.org/wiki/Symetrick%C3%A1_%C5%A1ifra

[20] Asymetrická kryptografie. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2015-04-04]. Dostupné z: http://cs.wikipedia.org/wiki/Asymetrick%C3%A1_kryptografie

[21] IEEE 802.1X. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2015-04-04]. Dostupné z: http://cs.wikipedia.org/wiki/IEEE_802.1X

[22] Wi-Fi Security. [online]. [cit. 2015-04-04]. Dostupné z: http://www.rhyshaden.com/wifisec.htm

[23] LinSSID. [online]. [cit. 2015-04-04]. Dostupné z: http://sourceforge.net/projects/linssid/

[24] InSSIDer by MetaGeek. [online]. [cit. 2015-04-04]. Dostupné z: http://www.inssider.com/?utm_expid=80366919-52.xFTKjY6_QkGzl57I2-Qj1g.0&utm_referrer=https%3A%2F%2Fwww.google.cz%2F

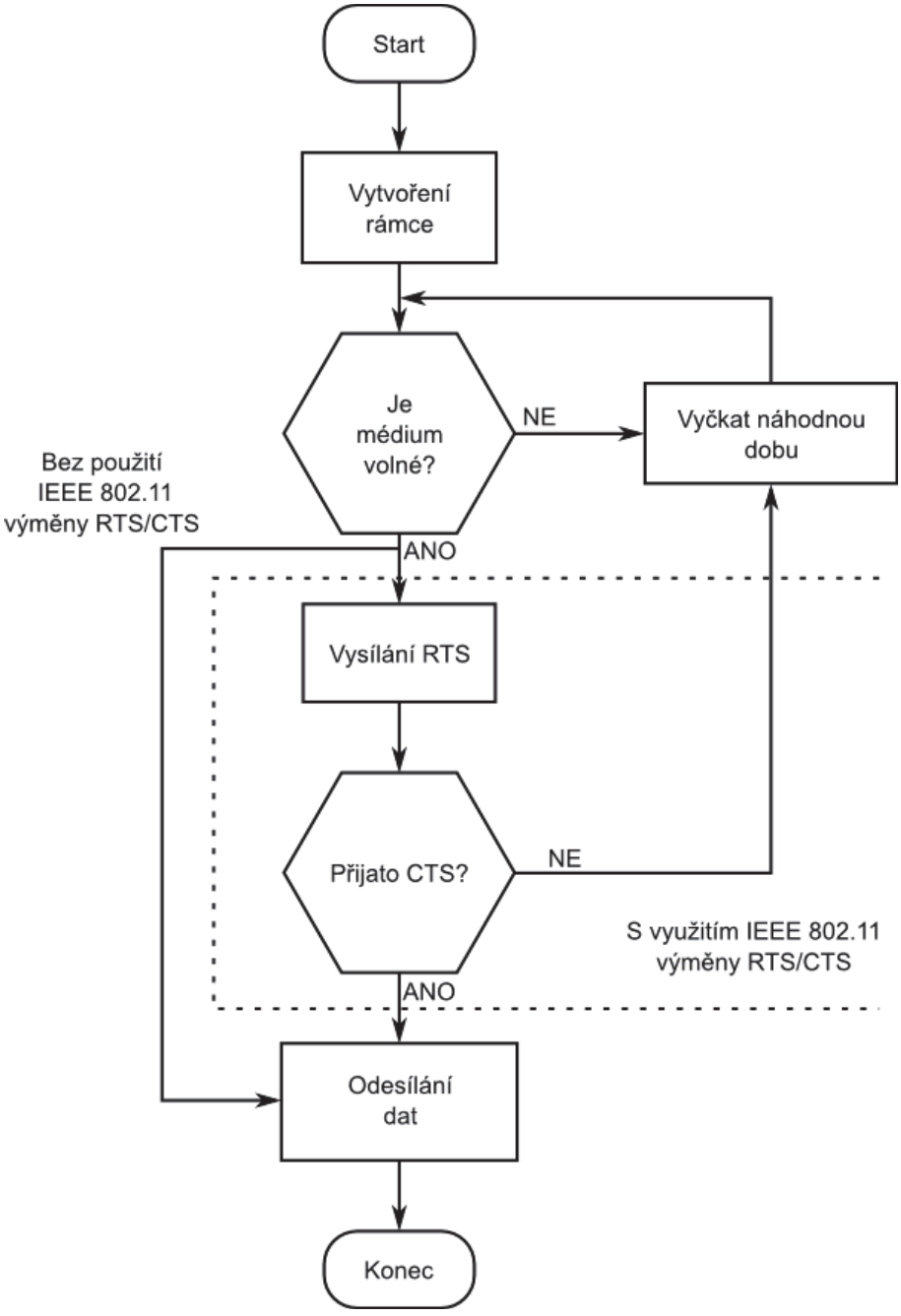
[25] OREBAUGH, Angela, *Wireshark a Ethereal: kompletní průvodce analýzou a diagnostikou sítí*, Vyd. 1. Brno: Computer Press, 2008, 444 s. ISBN 978-80-251-2048-4

[26] Wireshark. [online]. [cit. 2015-04-24]. Dostupné z: https://www.wireshark.org/

[27] IEEE 802.11i-2004: The Four-Way Handshake. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2015-04-25]. Dostupné z: http://en.wikipedia.org/wiki/IEEE_802.11i-2004

Seznam příloh

A Schéma - princip CSMA/CA



Obrázek A.1: Princip CSMA/CA [8]